Qualys. Enterprise TruRisk™ Platform

Scan Results

January 08, 2026

Report Summary	
User Name:	Joseph Fackler
Login Name:	pwerm3sf
Company:	Power Monitors Inc.
User Role:	Manager
Address:	800 North Main Street
City:	Mount Crawford
Country:	United States of America
Created:	01/08/2026 at 02:50:52 PM (GMT-0500)
Launch Date:	01/07/2026 at 05:24:07 PM (GMT-0500)
Active Hosts:	7
Total Hosts:	7
Type:	On demand
Status:	Finished
Reference:	scan/1767824647.52376
External Scanners:	64.39.98.77 (Scanner 14.13.6-1, Vulnerability Signatures 2.6.509-3)
Duration:	00:49:26
Title:	Weekly PQ Scan - 20260107
Asset Groups:	PQ
IPs:	34.195.90.152, 52.0.42.168
Excluded IPs:	-
FQDNs:	ai.powermonitors.com, fpl.powermonitors.com, pqcanvass.powermonitors.com, pqcanvasswebcommd.powermonitors.com, pqrecordings.powermonitors.com
Options Profile:	PMIa

Summary of Vulnerabilities

Vulnerabilities Total	93

Security Risk (Avg)	2.0

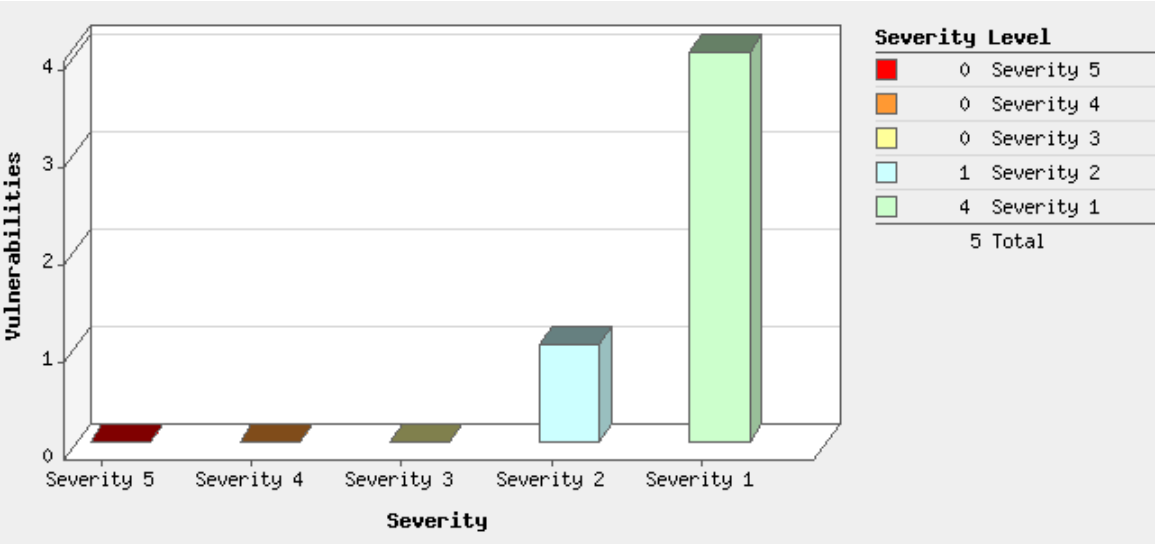
by Severity

Severity	Confirmed	Potential	Information Gathered	Total
5	0	0	0	0
4	0	0	0	0
3	0	2	2	4
2	1	0	5	6
1	4	0	79	83
Total	5	2	86	93

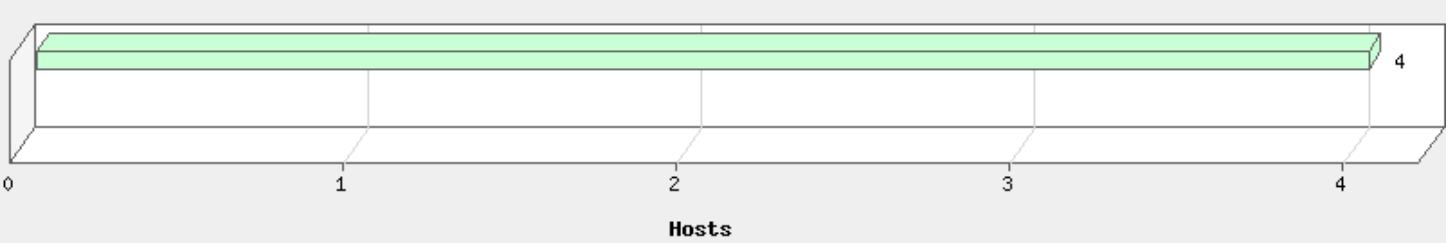
5 Biggest Categories

Category	Confirmed	Potential	Information Gathered	Total
Information gathering	0	0	35	35
TCP/IP	4	1	16	21
General remote services	0	0	21	21
Web server	0	1	7	8
Firewall	0	0	4	4
Total	4	2	83	89

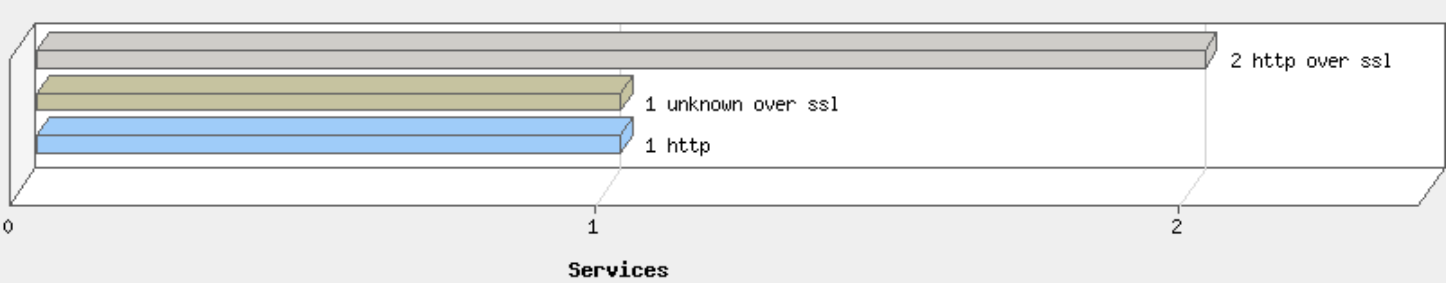
Vulnerabilities by Severity



Operating Systems Detected



Services Detected



Detailed Results

18.213.6.228 (pqcanvasswebcommd.powermonitors.com, -)

Vulnerabilities (1)

1 ICMP Timestamp Request

QID:	82003
Category:	TCP/IP
Associated CVEs:	CVE-1999-0524
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/28/2025
User Modified:	-

Edited:	No
PCI Vuln:	No

THREAT:

ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. It's principal purpose is to provide a protocol layer able to inform gateways of the inter-connectivity and accessibility of other gateways or hosts. "ping" is a well-known program for determining if a host is up or down. It uses ICMP echo packets.

ICMP timestamp packets are used to synchronize clocks between hosts. Revealing the current time on the system may facilitate attackers to mount further attacks. Since the risk is especially high on internet facing targets, this vulnerability will be flagged only be Internet scanners hosted by Qualys. Internal targets will not be flagged with this vulnerability.

Please see QID:82040 for a list of supported ICMP packet types.

IMPACT:

Unauthorized users can obtain information about your network by sending ICMP timestamp packets. For example, the internal systems clock should not be disclosed since some internal daemons use this value to calculate ID or sequence numbers (i.e., on SunOS servers).

SOLUTION:

You can filter ICMP messages of type "Timestamp" and "Timestamp Reply" at the firewall level. Some system administrators choose to filter most types of ICMP messages for various reasons. For example, they may want to protect their internal hosts from ICMP-based Denial Of Service attacks, such as the Ping of Death or Smurf attacks.

However, you should never filter ALL ICMP messages, as some of them ("Don't Fragment", "Destination Unreachable", "Source Quench", etc) are necessary for proper behavior of Operating System TCP/IP stacks.

It may be wiser to contact your network consultants for advice, since this issue impacts your overall network reliability and security.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

github-exploits

Reference:	CVE-1999-0524
Description:	threatlabindonesia/CVE-1999-0524-ICMP-Timestamp-and-Address-Mask-Request-Exploit exploit repository
Link:	https://github.com/threatlabindonesia/CVE-1999-0524-ICMP-Timestamp-and-Address-Mask-Request-Exploit

Reference:	CVE-1999-0524
Description:	Ransc0rp1on/ICMP-Timestamp-POC exploit repository
Link:	https://github.com/Ransc0rp1on/ICMP-Timestamp-POC

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Timestamp of host (network byte ordering): 22:25:29 GMT

Potential Vulnerabilities (1)

3 Web Server Stopped Responding — port 443/tcp over SSL

QID:	86476
Category:	Web server
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/27/2023
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

The Web server stopped responding to 3 consecutive connection attempts and/or more than 3 consecutive HTTP / HTTPS requests. Consequently, the service aborted testing for HTTP / HTTPS vulnerabilities. The vulnerabilities already detected are still posted.

For more details about this QID, please review the following Qualys KB article:
Qualys KB (https://success.qualys.com/support/s/article/000003057)

IMPACT:

The service was unable to complete testing for HTTP / HTTPS vulnerabilities since the Web server stopped responding.

SOLUTION:

Check the Web server status.

If the Web server was crashed during the scan, please restart the server, report the incident to Customer Support and stop scanning the Web server until the issue is resolved.

If the Web server is unable to process multiple concurrent HTTP / HTTPS requests, please lower the scan harshness level and launch another scan. If this vulnerability continues to be reported, please contact Customer Support.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

The web server did not respond for 4 consecutive HTTP requests.

Information Gathered (26)

2 Host Uptime Based on TCP TimeStamp Option

QID:	82063
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/29/2007
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The TCP/IP stack on the host supports the TCP TimeStamp (kind 8) option. Typically the timestamp used is the host's uptime (since last reboot) in various units (e.g., one hundredth of second, one tenth of a second, etc.). Based on this, we can obtain the host's uptime. The result is given in the Result section below.

Some operating systems (e.g., MacOS, OpenBSD) use a non-zero, probably random, initial value for the timestamp. For these operating systems, the uptime obtained does not reflect the actual uptime of the host; the former is always larger than the latter.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Based on TCP timestamps obtained via port 443, the host's uptime is 33 days, 9 hours, and 51 minutes.
The TCP timestamps from the host are in units of 1 milliseconds.

1 DNS Host Name

QID:	6
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/04/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

IP address	Host name
18.213.6.228	pqcanvasswebcommd.powermonitors.com
18.213.6.228	ec2-18-213-6-228.compute-1.amazonaws.com

1 Firewall Detected

QID:	34011
Category:	Firewall
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/21/2019
User Modified:	-

Edited:	No
PCI Vuln:	No

THREAT:

A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Some of the ports filtered by the firewall are: 20, 21, 22, 23, 25, 53, 80, 111, 135, 445.

Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
1-381,383-442,445-6128,6130-6442,6444-11016,11018-11019,11021-24476,24478-45458,
45460-65535

1 Target Network Information

QID:	45004
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/15/2013
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).

This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

IMPACT:

This information can be used by malicious users to gather more information about the network infrastructure that may help in launching attacks against it.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

The network handle is: AT-88-Z
Network description:
Amazon Technologies Inc.

1 Internet Service Provider

QID:	45005
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/27/2013
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).

This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

IMPACT:

This information can be used by malicious users to gather more information about the network infrastructure that may aid in launching further attacks against it.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

The ISP network handle is: LVLT-ORG-4-8
ISP Network description:
Level 3 Parent, LLC

1 Traceroute

QID:	45006
Category:	Information gathering
Associated CVEs:	-

Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/09/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Traceroute describes the path in realtime from the scanner to the remote host being contacted. It reports the IP addresses of all the routers in between.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Hops	IP	Round Trip Time	Probe	Port
1	139.87.10.24	0.76ms	ICMP	
2	4.15.10.202	0.44ms	ICMP	
3	4.15.10.201	1.07ms	ICMP	
4	4.69.219.218	2.34ms	ICMP	
5	*.*.*.*	0.00ms	Other	443
6	*.*.*.*	0.00ms	Other	443
7	*.*.*.*	0.00ms	Other	443
8	*.*.*.*	0.00ms	Other	443
9	*.*.*.*	0.00ms	Other	443
10	18.213.6.228	55.60ms	ICMP	

1 Host Scan Time - Scanner

QID:	45038
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/15/2022
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.

The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Scan duration: 1263 seconds

Start time: Wed, Jan 07 2026, 22:25:26 GMT

End time: Wed, Jan 07 2026, 22:46:29 GMT

 1 Host Names Found

QID:	45039
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/26/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Host Name	Source
pqcanvasswebcommd.powermonitors.com	User-provided DNS

1 Scan Activity per Port

QID:	45426
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/24/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Scan activity per port is an estimate of the amount of internal process time the scanner engine spent scanning a particular TCP or UDP port. This information can be useful to determine the reason for long scan times. The individual time values represent internal process time, not elapsed time, and can be longer than the total scan time because of internal parallelism. High values are often caused by slowly responding services or services on which requests time out.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Protocol	Port	Time
TCP	443	0:06:45
TCP	6443	0:15:13
TCP	11017	0:10:27
TCP	11020	0:03:10
TCP	45459	0:08:57

1 Open TCP Services List

QID:	82023
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/19/2025
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.

The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
443	https	http protocol over TLS/SSL	http over ssl	
6443	unknown	unknown	unknown over ssl	
11017	unknown	unknown	unknown	
11020	unknown	unknown	unknown	
45459	unknown	unknown	unknown	

1 ICMP Replies Received

QID:	82040
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.

We have sent the following types of packets to trigger the host to send us ICMP replies:

Echo Request (to trigger Echo Reply)
Timestamp Request (to trigger Timestamp Reply)
Address Mask Request (to trigger Address Mask Reply)
UDP Packet (to trigger Port Unreachable Reply)
IP Packet with Protocol >= 250 (to trigger Protocol Unreachable Reply)

Listed in the "Result" section are the ICMP replies that we have received.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

ICMP Reply Type	Triggered By	Additional Information
Echo (type=0 code=0)	Echo Request	Echo Reply
Time Stamp (type=14 code=0)	Time Stamp Request	22:25:29 GMT

1 Degree of Randomness of TCP Initial Sequence Numbers

QID:	82045
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/19/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

TCP Initial Sequence Numbers (ISNs) obtained in the SYNACK replies from the host are analyzed to determine how random they are. The average change between subsequent ISNs and the standard deviation from the average are displayed in the RESULT section. Also included is the degree of difficulty for exploitation of the TCP ISN generation scheme used by the host.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Average change between subsequent TCP initial sequence numbers is 1189563458 with a standard deviation of 593502205. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(5107 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is: hard.

1 IP ID Values Randomness

QID:	82046
Category:	TCP/IP

Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/27/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The values for the identification (ID) field in IP headers in IP packets from the host are analyzed to determine how random they are. The changes between subsequent ID values for either the network byte ordering or the host byte ordering, whichever is smaller, are displayed in the RESULT section along with the duration taken to send the probes. When incremental values are used, as is the case for TCP/IP implementation in many operating systems, these changes reflect the network load of the host at the time this test was conducted.

Please note that for reliability reasons only the network traffic from open TCP ports is analyzed.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

IP ID changes observed (network order) for port 443: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Duration: 33 milli seconds

1 SSL Server Information Retrieval — port 443/tcp over SSL

QID:	38116
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.

Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
ECDHE-ECDSA-AES256-GCM-SHA384	ECDH	ECDSA	AEAD	AESGCM(256)	HIGH
ECDHE-ECDSA-CHACHA20-POLY1305	ECDH	ECDSA	AEAD	CHACHA20/POLY1305(256)	HIGH
TLSv1.3 PROTOCOL IS ENABLED					
TLS13-AES-256-GCM-SHA384	N/A	N/A	AEAD	AESGCM(256)	HIGH

1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance port 443/tcp over SSL

QID:	38597
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	rejected
0399	rejected
0400	rejected
0499	0303

1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods port 443/tcp over SSL

QID:	38704
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/01/2023
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes, strengths and ciphers.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2						
ECDHE-ECDSA-CHACHA20-POLY1305	ECDHE	x25519	256	yes	128	low
TLSv1.3						
TLS13-AES-256-GCM-SHA384	ECDHE	x25519	256	yes	128	low

1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties port 443/tcp over SSL

QID:	38706
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/09/2021

User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The following is a list of detected SSL/TLS protocol properties.

IMPACT:

Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Heartbeat	no
OCSP stapling	no
SCT extension	no
TLSv1.3	
Heartbeat	no
OCSP stapling	no
SCT extension	no

1 SSL Server Information Retrieval port 6443/tcp over SSL

QID: 38116
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 05/24/2016
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The following is a list of supported SSL ciphers.

Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
ECDHE-ECDSA-AES128-SHA	ECDH	ECDSA	SHA1	AES(128)	MEDIUM
ECDHE-ECDSA-AES256-SHA	ECDH	ECDSA	SHA1	AES(256)	HIGH
ECDHE-ECDSA-AES128-SHA256	ECDH	ECDSA	SHA256	AES(128)	MEDIUM
ECDHE-ECDSA-AES256-SHA384	ECDH	ECDSA	SHA384	AES(256)	HIGH
ECDHE-ECDSA-AES128-GCM-SHA256	ECDH	ECDSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-ECDSA-AES256-GCM-SHA384	ECDH	ECDSA	AEAD	AESGCM(256)	HIGH
ECDHE-ECDSA-CHACHA20-POLY1305	ECDH	ECDSA	AEAD	CHACHA20/POLY1305(256)	HIGH
TLSv1.3 PROTOCOL IS ENABLED					
TLS13-AES-128-GCM-SHA256	N/A	N/A	AEAD	AESGCM(128)	MEDIUM
TLS13-AES-256-GCM-SHA384	N/A	N/A	AEAD	AESGCM(256)	HIGH
TLS13-CHACHA20-POLY1305-SHA256	N/A	N/A	AEAD	CHACHA20/POLY1305(256)	HIGH

1 SSL Session Caching Information port 6443/tcp over SSL

QID:	38291
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No

PCI Vuln: No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.

This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is disabled on the target.
TLSv1.3 session caching is disabled on the target.

 1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance port 6443/tcp over SSL

QID:	38597
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

1 SSL Certificate will expire within next six months port 6443/tcp over SSL

QID:	38600
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/14/2024
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Certificates are used for authentication purposes in different protocols such as SSL/TLS. Each certificate has a validity period outside of which it is supposed to be considered invalid. This QID is reported to inform that a certificate will expire within next six months. The advance notice can be helpful since obtaining a certificate can take some time.

IMPACT:

Expired certificates can cause connection disruptions or compromise the integrity and privacy of the connections being protected by the certificates.

SOLUTION:

Contact the certificate authority that signed your certificate to arrange for a renewal.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Certificate #0 CN=*.powermonitors.com The certificate will expire within six months: Mar 5 17:31:54 2026 GMT

1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods port 6443/tcp over SSL

QID:	38704

Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/01/2023
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes, strengths and ciphers.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2						
ECDHE-ECDSA-AES256-GCM-SHA384	ECDHE	x448	448	yes	224	low
ECDHE-ECDSA-AES256-GCM-SHA384	ECDHE	x25519	256	yes	128	low
ECDHE-ECDSA-AES256-GCM-SHA384	ECDHE	secp384r1	384	yes	192	low
ECDHE-ECDSA-AES256-GCM-SHA384	ECDHE	secp256r1	256	yes	128	low
ECDHE-ECDSA-CHACHA20-POLY1305	ECDHE	x448	448	yes	224	low
ECDHE-ECDSA-CHACHA20-POLY1305	ECDHE	x25519	256	yes	128	low
ECDHE-ECDSA-CHACHA20-POLY1305	ECDHE	secp384r1	384	yes	192	low
ECDHE-ECDSA-CHACHA20-POLY1305	ECDHE	secp256r1	256	yes	128	low
ECDHE-ECDSA-AES128-GCM-SHA256	ECDHE	x448	448	yes	224	low
ECDHE-ECDSA-AES128-GCM-SHA256	ECDHE	x25519	256	yes	128	low
ECDHE-ECDSA-AES128-GCM-SHA256	ECDHE	secp384r1	384	yes	192	low
ECDHE-ECDSA-AES128-GCM-SHA256	ECDHE	secp256r1	256	yes	128	low
ECDHE-ECDSA-AES256-SHA384	ECDHE	x448	448	yes	224	low
ECDHE-ECDSA-AES256-SHA384	ECDHE	x25519	256	yes	128	low
ECDHE-ECDSA-AES256-SHA384	ECDHE	secp384r1	384	yes	192	low
ECDHE-ECDSA-AES256-SHA384	ECDHE	secp256r1	256	yes	128	low
ECDHE-ECDSA-AES128-SHA256	ECDHE	x448	448	yes	224	low

ECDHE-ECDSA-AES128-SHA256	ECDHE	x25519	256	yes	128	low
ECDHE-ECDSA-AES128-SHA256	ECDHE	secp384r1	384	yes	192	low
ECDHE-ECDSA-AES128-SHA256	ECDHE	secp256r1	256	yes	128	low
ECDHE-ECDSA-AES256-SHA	ECDHE	x448	448	yes	224	low
ECDHE-ECDSA-AES256-SHA	ECDHE	x25519	256	yes	128	low
ECDHE-ECDSA-AES256-SHA	ECDHE	secp384r1	384	yes	192	low
ECDHE-ECDSA-AES256-SHA	ECDHE	secp256r1	256	yes	128	low
ECDHE-ECDSA-AES128-SHA	ECDHE	x448	448	yes	224	low
ECDHE-ECDSA-AES128-SHA	ECDHE	x25519	256	yes	128	low
ECDHE-ECDSA-AES128-SHA	ECDHE	secp384r1	384	yes	192	low
ECDHE-ECDSA-AES128-SHA	ECDHE	secp256r1	256	yes	128	low
TLSv1.3						
TLS13-AES-128-GCM-SHA256	ECDHE	x25519	256	yes	128	low
TLS13-AES-128-GCM-SHA256	ECDHE	secp256r1	256	yes	128	low
TLS13-AES-128-GCM-SHA256	ECDHE	x448	448	yes	224	low
TLS13-AES-128-GCM-SHA256	ECDHE	secp521r1	521	yes	260	low
TLS13-AES-128-GCM-SHA256	ECDHE	secp384r1	384	yes	192	low
TLS13-AES-256-GCM-SHA384	ECDHE	x25519	256	yes	128	low
TLS13-AES-256-GCM-SHA384	ECDHE	secp256r1	256	yes	128	low
TLS13-AES-256-GCM-SHA384	ECDHE	x448	448	yes	224	low
TLS13-AES-256-GCM-SHA384	ECDHE	secp521r1	521	yes	260	low
TLS13-AES-256-GCM-SHA384	ECDHE	secp384r1	384	yes	192	low
TLS13-CHACHA20-POLY1305-SHA256	ECDHE	x25519	256	yes	128	low
TLS13-CHACHA20-POLY1305-SHA256	ECDHE	secp256r1	256	yes	128	low
TLS13-CHACHA20-POLY1305-SHA256	ECDHE	x448	448	yes	224	low
TLS13-CHACHA20-POLY1305-SHA256	ECDHE	secp521r1	521	yes	260	low
TLS13-CHACHA20-POLY1305-SHA256	ECDHE	secp384r1	384	yes	192	low

1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties port 6443/tcp over SSL

QID:	38706
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/09/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of detected SSL/TLS protocol properties.

IMPACT:

Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	yes
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	client
OCSP stapling	no
SCT extension	no
TLSv1.3	
Heartbeat	no
Cipher priority controlled by	client
OCSP stapling	no
SCT extension	no

1 Secure Sockets Layer (SSL) Certificate Transparency Information port 6443/tcp over SSL

QID:	38718
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/08/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".

The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.powermonitors .com			
Certificate	no	(unknown)	(unknown)	969764bf555897adf743876837084277e9f03 ad5f6a4f3366e46a43f0fcaa9c6	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	no	(unknown)	(unknown)	16832dabf0a9250f0ff03aa545ffc8bfc823d 0874bf6042927f8e71f3313f5fa	Thu 01 Jan 1970 12:00:00 AM GMT

1 TLS Secure Renegotiation Extension Support Information port 6443/tcp over SSL

QID:	42350
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.

1 SSL Certificate - Information port 6443/tcp over SSL

QID:	86002
Category:	Web server
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL certificate information is provided in the Results section.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	06:1a:09:42:b1:49:03:b3:89:94:da:64:ae:88:e1:7b:a5:58
(0)Signature Algorithm	ecdsa-with-SHA384
(0)ISSUER NAME	
countryName	US
organizationName	Let's Encrypt
commonName	E8
(0)SUBJECT NAME	
commonName	*.powermonitors.com
(0)Valid From	Dec 5 17:31:55 2025 GMT
(0)Valid Till	Mar 5 17:31:54 2026 GMT
(0)Public Key Algorithm	id-ecPublicKey
(0)EC Public Key	
(0)	Public-Key: (256 bit)
(0)	pub:
(0)	04:72:6f:9e:3f:16:3f:dc:69:cf:d0:e1:27:58:47:
(0)	d9:0c:04:61:da:bd:c1:47:b4:4e:ee:87:84:a1:3a:

(0)	77:38:9a:dc:95:7e:53:40:cd:a9:df:6c:94:6b:18:
(0)	1b:81:06:20:04:13:63:b8:a6:a7:d8:bc:ba:be:81:
(0)	da:93:92:ba:46
(0)	ASN1 OID: prime256v1
(0)	NIST CURVE: P-256
(0)X509v3 EXTENSIONS	
(0)X509v3 Key Usage	critical
(0)	Digital Signature
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Subject Key Identifier	2C:41:DF:56:C1:E5:C4:BD:24:96:B6:6B:6C:A8:2C:7D:35:37:B1:2A
(0)X509v3 Authority Key Identifier	keyid:8F:0D:13:A2:F6:2E:7E:D1:50:6C:33:18:38:5D:59:8E:23:72:91:CA
(0)Authority Information Access	CA Issuers - URI:http://e8.i.lencr.org/
(0)X509v3 Subject Alternative Name	DNS:*.powermonitors.com
(0)X509v3 Certificate Policies	Policy: 2.23.140.1.2.1
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://e8.c.lencr.org/89.crl
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 96:97:64:BF:55:58:97:AD:F7:43:87:68:37:08:42:77:
(0)	E9:F0:3A:D5:F6:A4:F3:36:6E:46:A4:3F:0F:CA:A9:C6
(0)	Timestamp : Dec 5 18:30:25.927 2025 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:21:00:87:CF:16:8C:25:0F:E2:B8:95:2F:25:
(0)	41:EA:34:9F:95:FA:7D:A6:A3:2D:A7:59:4B:F4:E2:50:
(0)	83:27:6B:60:5C:02:20:69:29:D8:2F:D2:FC:29:8D:FE:
(0)	FE:AA:32:2D:FE:70:40:72:FE:F9:D3:45:46:2B:20:EE:
(0)	8F:29:A8:EE:E9:D0:22
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 16:83:2D:AB:F0:A9:25:0F:0F:F0:3A:A5:45:FF:C8:BF:
(0)	C8:23:D0:87:4B:F6:04:29:27:F8:E7:1F:33:13:F5:FA
(0)	Timestamp : Dec 5 18:30:28.436 2025 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:21:00:93:00:22:B4:ED:B1:DC:E8:18:9F:7A:
(0)	98:FC:74:69:A9:30:D8:81:5F:4D:56:0F:7B:3A:58:08:
(0)	A3:75:49:38:91:02:20:72:F4:5D:AC:55:0D:32:BE:87:
(0)	4D:C1:88:12:84:A8:4E:3D:23:BC:E0:34:20:86:4D:2D:
(0)	07:2B:95:DE:69:AB:34
(0)Signature	(103 octets)
(0)	30:65:02:30:0c:b0:8d:fe:38:12:07:30:c8:2c:bb:66
(0)	da:66:a6:38:83:08:9b:23:a5:0c:9f:db:22:5c:9e:7b
(0)	fd:fb:1e:47:04:01:80:81:f5:6e:92:35:c7:fb:0d:87
(0)	6d:e6:8e:d9:02:31:00:c9:c2:81:03:55:39:43:b7:03
(0)	8e:3a:b1:97:31:df:e7:58:be:42:e4:21:00:7b:63:a1
(0)	9c:ef:59:ba:96:a4:3c:b6:d4:7f:df:43:ad:fa:5e:d8
(0)	e2:3a:6c:43:b0:ef:da:00
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	63:95:93:63:c2:4e:70:82:71:59:18:bf:c3:d7:ed:56
(1)Signature Algorithm	sha256WithRSAEncryption

(1)ISSUER NAME	
countryName	US
organizationName	Internet Security Research Group
commonName	ISRG Root X1
(1)SUBJECT NAME	
countryName	US
organizationName	Let's Encrypt
commonName	E8
(1)Valid From	Mar 13 00:00:00 2024 GMT
(1)Valid Till	Mar 12 23:59:59 2027 GMT
(1)Public Key Algorithm	id-ecPublicKey
(1)EC Public Key	
(1)	Public-Key: (384 bit)
(1)	pub:
(1)	04:d1:65:f2:5e:dc:4b:b4:0c:02:9c:d2:b2:fa:ee:
(1)	e9:6c:ab:3a:ae:38:a1:f4:d4:39:32:33:c5:42:d4:
(1)	cc:33:0c:34:c7:21:20:90:70:5c:e8:62:2f:1c:71:
(1)	b3:42:d7:79:be:46:0d:c1:db:47:a1:13:a0:c7:df:
(1)	81:26:63:3b:d4:8d:1d:f6:3d:82:33:32:f6:f4:2b:
(1)	e7:f5:96:3a:b4:13:67:18:7b:6b:3e:8d:48:d9:ea:
(1)	de:ed:ae:6d:3e:87:4c
(1)	ASN1 OID: secp384r1
(1)	NIST CURVE: P-384
(1)X509v3 EXTENSIONS	
(1)X509v3 Key Usage	critical
(1)	Digital Signature, Certificate Sign, CRL Sign
(1)X509v3 Extended Key Usage	TLS Web Client Authentication, TLS Web Server Authentication
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE, pathlen:0
(1)X509v3 Subject Key Identifier	8F:0D:13:A2:F6:2E:7E:D1:50:6C:33:18:38:5D:59:8E:23:72:91:CA
(1)X509v3 Authority Key Identifier	keyid:79:B4:59:E6:7B:B6:E5:E4:01:73:80:08:88:C8:1A:58:F6:E9:9B:6E
(1)Authority Information Access	CA Issuers - URI:http://x1.i.lencr.org/
(1)X509v3 Certificate Policies	Policy: 2.23.140.1.2.1
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://x1.c.lencr.org/
(1)Signature	(512 octets)
(1)	67:13:48:46:20:d2:ac:09:85:a2:d1:7c:75:ca:0c:43
(1)	e6:a8:a1:12:36:74:44:8d:ed:4d:9c:f5:c2:e0:13:1f
(1)	76:70:60:f2:29:f7:b9:16:11:ac:9a:9c:3d:63:d1:c0
(1)	e1:21:8c:f2:e0:29:03:a3:68:c1:f0:3e:6d:d1:ae:b3
(1)	65:6c:e5:af:df:1d:01:01:4d:87:cb:8a:26:42:07:74
(1)	b4:a1:cb:e9:d4:c9:e6:71:73:96:cd:78:ca:75:2e:ed
(1)	20:4b:31:38:31:ca:9f:98:d3:2f:22:97:a2:c1:64:98
(1)	3b:dc:3c:d8:e6:fc:a2:db:d7:70:ed:89:51:88:b7:b2
(1)	f1:c8:59:19:b7:fb:bd:3b:0d:46:cb:e7:55:cc:71:8d
(1)	a2:65:d9:42:ab:85:9a:f6:76:ee:93:75:93:53:88:2b
(1)	e8:b6:3c:33:35:40:68:34:06:db:ee:14:dd:e2:7a:a9
(1)	41:75:d1:b0:67:47:5b:ae:57:20:d8:b3:d4:61:af:0b
(1)	9c:45:59:df:b8:38:f6:f4:23:0b:4e:ca:65:33:97:f9
(1)	c1:25:79:85:4a:66:53:0a:7f:bd:5e:cc:e3:0e:1a:1a
(1)	e9:ed:ef:89:28:5f:bd:67:e0:47:5a:80:2b:0b:fd:89
(1)	39:fa:60:10:53:4f:ad:b9:ed:09:39:f0:15:fd:1e:ad
(1)	d6:4f:97:93:db:36:1c:c4:05:7a:8c:69:a5:fc:c0:54
(1)	2d:38:15:d1:bd:33:e0:02:d8:95:b1:98:54:ad:e8:10

(1)	ae:87:70:84:7b:2d:df:13:9d:90:ae:3f:58:33:be:6b
(1)	b6:f2:23:b2:6f:f5:1e:5f:ae:ff:f5:aa:c6:7b:b5:65
(1)	0e:23:a5:af:95:a6:e6:62:18:e9:56:ae:a4:8f:f5:ea
(1)	20:74:e8:42:1a:2b:27:c9:ec:16:27:04:50:3a:a2:b5
(1)	eb:08:86:c9:97:91:c6:cf:c1:7a:4c:3a:e6:fc:12:21
(1)	a5:64:06:bb:8f:89:37:cc:3a:8d:19:87:88:15:6b:cf
(1)	ea:26:03:1b:25:bc:ab:c3:01:bd:ef:3f:cf:46:09:8b
(1)	28:20:e5:f3:3d:dd:b4:0d:19:ee:aa:bb:7e:d6:b4:1a
(1)	5d:b8:bb:2b:81:d3:97:6a:23:92:75:2e:f0:33:2a:e5
(1)	9d:22:34:f5:b4:ff:2a:0a:8c:52:13:fc:69:8b:1f:21
(1)	5f:67:6d:de:1f:bf:8e:e8:d4:80:53:c5:67:41:15:67
(1)	4c:52:c8:13:51:17:73:1b:a0:66:67:61:71:54:c6:93
(1)	63:4d:63:ca:a5:a8:03:1c:94:26:aa:b0:1c:0e:65:89
(1)	9c:cb:05:63:78:d2:bb:58:a0:bf:73:9e:7e:75:a3:49

34.195.90.152 (ec2-34-195-90-152.compute-1.amazonaws.com, -)

Vulnerabilities (1)

1 ICMP Timestamp Request

QID:	82003
Category:	TCP/IP
Associated CVEs:	CVE-1999-0524
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/28/2025
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. It's principal purpose is to provide a protocol layer able to inform gateways of the inter-connectivity and accessibility of other gateways or hosts. "ping" is a well-known program for determining if a host is up or down. It uses ICMP echo packets.

ICMP timestamp packets are used to synchronize clocks between hosts. Revealing the current time on the system may facilitate attackers to mount further attacks. Since the risk is especially high on internet facing targets, this vulnerability will be flagged only be Internet scanners hosted by Qualys. Internal targets will not be flagged with this vulnerability.

Please see QID:82040 for a list of supported ICMP packet types.

IMPACT:

Unauthorized users can obtain information about your network by sending ICMP timestamp packets. For example, the internal systems clock should not be disclosed since some internal daemons use this value to calculate ID or sequence numbers (i.e., on SunOS servers).

SOLUTION:

You can filter ICMP messages of type "Timestamp" and "Timestamp Reply" at the firewall level. Some system administrators choose to filter most types of ICMP messages for various reasons. For example, they may want to protect their internal hosts from ICMP-based Denial Of Service attacks, such as the Ping of Death or Smurf attacks.

However, you should never filter ALL ICMP messages, as some of them ("Don't Fragment", "Destination Unreachable", "Source Quench", etc) are necessary for proper behavior of Operating System TCP/IP stacks.

It may be wiser to contact your network consultants for advice, since this issue impacts your overall network reliability and security.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

github-exploits

Reference: CVE-1999-0524
Description: threatlabindonesia/CVE-1999-0524-ICMP-Timestamp-and-Address-Mask-Request-Exploit exploit repository
Link: https://github.com/threatlabindonesia/CVE-1999-0524-ICMP-Timestamp-and-Address-Mask-Request-Exploit

Reference: CVE-1999-0524
Description: Ransc0rp1on/ICMP-Timestamp-POC exploit repository
Link: https://github.com/Ransc0rp1on/ICMP-Timestamp-POC

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Timestamp of host (network byte ordering): 22:25:44 GMT

Information Gathered (8)

1 DNS Host Name

QID:	6
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/04/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

IP address	Host name
34.195.90.152	ec2-34-195-90-152.compute-1.amazonaws.com

1 Firewall Detected

QID:	34011

Category:	Firewall
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/21/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
1-381,383-442,445-1559,1561-1705,1707-1721,1723-1999,2001-2033,2035,2037-2100,
2102-2146,2148-2512,2514-2701,2703-3388,3390-5491,5493-5504,5506-5549,
5551-5559,5561-5569,5571-5579,5581-5630,5632-6013,6015-6128,6130-6442,
6444-7006,7008-7009,7011-9098,9100-9989,9991-10109,10111-11016,11018-11019,
11021-24476,24478-42423,42425-45458,45460-65535

1 Target Network Information

QID:	45004
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/15/2013
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).

This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

IMPACT:

This information can be used by malicious users to gather more information about the network infrastructure that may help in launching attacks against it.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

The network handle is: AT-88-Z
Network description:
Amazon Technologies Inc.

 1 Internet Service Provider

QID:	45005
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/27/2013
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).

This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

IMPACT:

This information can be used by malicious users to gather more information about the network infrastructure that may aid in launching further attacks against it.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

The ISP network handle is: LVLT-ORG-4-8
ISP Network description:

Level 3 Parent, LLC

1 Traceroute

QID:	45006
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/09/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Traceroute describes the path in realtime from the scanner to the remote host being contacted. It reports the IP addresses of all the routers in between.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Hops	IP	Round Trip Time	Probe	Port
1	139.87.10.28	0.06ms	ICMP	
2	4.15.10.202	0.44ms	ICMP	
3	4.15.10.201	1.00ms	ICMP	
4	4.69.219.214	1.42ms	ICMP	
5	*.*.*.*	0.00ms	Other	80
6	*.*.*.*	0.00ms	Other	80
7	*.*.*.*	0.00ms	Other	80
8	*.*.*.*	0.00ms	Other	80
9	*.*.*.*	0.00ms	Other	80
10	34.195.90.152	55.62ms	ICMP	

1 Host Scan Time - Scanner

QID:	45038
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/15/2022
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.

The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Scan duration: 726 seconds

Start time: Wed, Jan 07 2026, 22:25:25 GMT

End time: Wed, Jan 07 2026, 22:37:31 GMT

 1 Host Names Found

QID:	45039
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/26/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Host Name	Source
ec2-34-195-90-152.compute-1.amazonaws.com	FQDN

1 ICMP Replies Received

QID:	82040
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.

We have sent the following types of packets to trigger the host to send us ICMP replies:

Echo Request (to trigger Echo Reply)
Timestamp Request (to trigger Timestamp Reply)
Address Mask Request (to trigger Address Mask Reply)
UDP Packet (to trigger Port Unreachable Reply)
IP Packet with Protocol >= 250 (to trigger Protocol Unreachable Reply)

Listed in the "Result" section are the ICMP replies that we have received.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

ICMP Reply Type	Triggered By	Additional Information
Echo (type=0 code=0)	Echo Request	Echo Reply
Time Stamp (type=14 code=0)	Time Stamp Request	22:25:44 GMT

52.0.42.168 (ec2-52-0-42-168.compute-1.amazonaws.com, -)

Vulnerabilities (1)

1 ICMP Timestamp Request

QID:	82003
Category:	TCP/IP
Associated CVEs:	CVE-1999-0524
Vendor Reference:	-

Bugtraq ID:	-
Service Modified:	05/28/2025
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. It's principal purpose is to provide a protocol layer able to inform gateways of the inter-connectivity and accessibility of other gateways or hosts. "ping" is a well-known program for determining if a host is up or down. It uses ICMP echo packets.

ICMP timestamp packets are used to synchronize clocks between hosts. Revealing the current time on the system may facilitate attackers to mount further attacks. Since the risk is especially high on internet facing targets, this vulnerability will be flagged only be Internet scanners hosted by Qualys. Internal targets will not be flagged with this vulnerability.

Please see QID:82040 for a list of supported ICMP packet types.

IMPACT:

Unauthorized users can obtain information about your network by sending ICMP timestamp packets. For example, the internal systems clock should not be disclosed since some internal daemons use this value to calculate ID or sequence numbers (i.e., on SunOS servers).

SOLUTION:

You can filter ICMP messages of type "Timestamp" and "Timestamp Reply" at the firewall level. Some system administrators choose to filter most types of ICMP messages for various reasons. For example, they may want to protect their internal hosts from ICMP-based Denial Of Service attacks, such as the Ping of Death or Smurf attacks.

However, you should never filter ALL ICMP messages, as some of them ("Don't Fragment", "Destination Unreachable", "Source Quench", etc) are necessary for proper behavior of Operating System TCP/IP stacks.

It may be wiser to contact your network consultants for advice, since this issue impacts your overall network reliability and security.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

github-exploits

Reference:	CVE-1999-0524
Description:	threatlabindonesia/CVE-1999-0524-ICMP-Timestamp-and-Address-Mask-Request-Exploit exploit repository
Link:	https://github.com/threatlabindonesia/CVE-1999-0524-ICMP-Timestamp-and-Address-Mask-Request-Exploit
Reference:	CVE-1999-0524
Description:	Ransc0rp1on/ICMP-Timestamp-POC exploit repository
Link:	https://github.com/Ransc0rp1on/ICMP-Timestamp-POC

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Timestamp of host (network byte ordering): 22:12:18 GMT

Information Gathered (13)

2 Host Uptime Based on TCP TimeStamp Option

QID:	82063
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/29/2007
User Modified:	-
Edited:	No

PCI Vuln: No

THREAT:

The TCP/IP stack on the host supports the TCP TimeStamp (kind 8) option. Typically the timestamp used is the host's uptime (since last reboot) in various units (e.g., one hundredth of second, one tenth of a second, etc.). Based on this, we can obtain the host's uptime. The result is given in the Result section below.

Some operating systems (e.g., MacOS, OpenBSD) use a non-zero, probably random, initial value for the timestamp. For these operating systems, the uptime obtained does not reflect the actual uptime of the host; the former is always larger than the latter.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Based on TCP timestamps obtained via port 11017, the host's uptime is 45 days, 14 hours, and 27 minutes.
The TCP timestamps from the host are in units of 1 milliseconds.

 1 DNS Host Name

QID: 6
Category: Information gathering
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 01/04/2018
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

IP address	Host name
52.0.42.168	ec2-52-0-42-168.compute-1.amazonaws.com

1 Firewall Detected

QID:	34011
Category:	Firewall
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/21/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Some of the ports filtered by the firewall are: 20, 21, 22, 23, 25, 53, 80, 111, 135, 445.

Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
1-381,383-442,445-6128,6130-6442,6444-11016,11018-11019,11021-24476,24478-45458,
45460-65535

1 Target Network Information

QID:	45004
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/15/2013
User Modified:	-
Edited:	No

PCI Vuln: No

THREAT:

The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).

This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

IMPACT:

This information can be used by malicious users to gather more information about the network infrastructure that may help in launching attacks against it.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

The network handle is: AT-88-Z
Network description:
Amazon Technologies Inc.

1 Internet Service Provider

QID:	45005
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/27/2013
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).

This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

IMPACT:

This information can be used by malicious users to gather more information about the network infrastructure that may aid in launching further attacks against it.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

The ISP network handle is: LVLT-ORG-4-8
ISP Network description:
Level 3 Parent, LLC

1 Traceroute

QID:	45006
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/09/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Traceroute describes the path in realtime from the scanner to the remote host being contacted. It reports the IP addresses of all the routers in between.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Hops	IP	Round Trip Time	Probe	Port
1	139.87.10.10	0.69ms	ICMP	
2	4.15.10.202	0.48ms	ICMP	
3	4.15.10.201	1.08ms	ICMP	
4	4.69.219.214	1.50ms	TCP	11017
5	*.*.*.*	0.00ms	Other	11017
6	*.*.*.*	0.00ms	Other	11017
7	*.*.*.*	0.00ms	Other	11017
8	*.*.*.*	0.00ms	Other	11017
9	*.*.*.*	0.00ms	Other	11017
10	52.0.42.168	61.57ms	TCP	11017

1 Host Scan Time - Scanner

QID:	45038

Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/15/2022
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.

The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Scan duration: 1515 seconds

Start time: Wed, Jan 07 2026, 22:25:25 GMT

End time: Wed, Jan 07 2026, 22:50:40 GMT

1 Host Names Found

QID:	45039
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/26/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Host Name	Source
ec2-52-0-42-168.compute-1.amazonaws.com	FQDN

 1 Scan Activity per Port

QID:	45426
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/24/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Scan activity per port is an estimate of the amount of internal process time the scanner engine spent scanning a particular TCP or UDP port. This information can be useful to determine the reason for long scan times. The individual time values represent internal process time, not elapsed time, and can be longer than the total scan time because of internal parallelism. High values are often caused by slowly responding services or services on which requests time out.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Protocol	Port	Time
TCP	11017	0:17:31

TCP	11020	0:04:08
TCP	45459	0:06:31

1 Open TCP Services List

QID:	82023
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/19/2025
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.

The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
11017	unknown	unknown	unknown	
11020	unknown	unknown	unknown	
45459	unknown	unknown	unknown	

1 ICMP Replies Received

QID:	82040
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.

We have sent the following types of packets to trigger the host to send us ICMP replies:

Echo Request (to trigger Echo Reply)
Timestamp Request (to trigger Timestamp Reply)
Address Mask Request (to trigger Address Mask Reply)
UDP Packet (to trigger Port Unreachable Reply)
IP Packet with Protocol >= 250 (to trigger Protocol Unreachable Reply)

Listed in the "Result" section are the ICMP replies that we have received.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

ICMP Reply Type	Triggered By	Additional Information
Echo (type=0 code=0)	Echo Request	Echo Reply
Time Stamp (type=14 code=0)	Time Stamp Request	22:12:18 GMT

 1 Degree of Randomness of TCP Initial Sequence Numbers

QID:	82045
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/19/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

TCP Initial Sequence Numbers (ISNs) obtained in the SYNACK replies from the host are analyzed to determine how random they are. The average change between subsequent ISNs and the standard deviation from the average are displayed in the RESULT section. Also included is the degree of difficulty for exploitation of the TCP ISN generation scheme used by the host.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Average change between subsequent TCP initial sequence numbers is 950640046 with a standard deviation of 728622460. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(5090 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is: hard.

1 IP ID Values Randomness

QID:	82046
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/27/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The values for the identification (ID) field in IP headers in IP packets from the host are analyzed to determine how random they are. The changes between subsequent ID values for either the network byte ordering or the host byte ordering, whichever is smaller, are displayed in the RESULT section along with the duration taken to send the probes. When incremental values are used, as is the case for TCP/IP implementation in many operating systems, these changes reflect the network load of the host at the time this test was conducted.

Please note that for reliability reasons only the network traffic from open TCP ports is analyzed.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

IP ID changes observed (network order) for port 11017: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Duration: 33 milli seconds

54.235.231.157 (fpl.powermonitors.com, -)

Vulnerabilities (2)

2 HTTP Security Header Not Detected port 443/tcp

QID:	11827
Category:	CGI
Associated CVEs:	-
Vendor Reference:	-

Bugtraq ID:	-
Service Modified:	01/02/2025
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

This QID reports the absence of the following HTTP headers (https://www.owasp.org/index.php/OWASP_Secure_Headers_Project#tab=Headers) according to CWE-693: Protection Mechanism Failure (https://cwe.mitre.org/data/definitions/693.html):

X-Content-Type-Options: This HTTP header will prevent the browser from interpreting files as a different MIME type to what is specified in the Content-Type HTTP header.
Strict-Transport-Security: The HTTP Strict-Transport-Security response header (HSTS) allows web servers to declare that web browsers (or other complying user agents) should only interact with it using secure HTTPS connections, and never via the insecure HTTP protocol.

IMPACT:

Depending on the vulnerability being exploited, an unauthenticated remote attacker could conduct cross-site scripting, clickjacking or MIME-type sniffing attacks.

SOLUTION:

Note: To better debug the results of this QID, it is requested that customers execute commands to simulate the following functionality: curl -IkL --verbose.

CWE-693: Protection Mechanism Failure mentions the following - The product does not use or incorrectly uses a protection mechanism that provides sufficient defense against directed attacks against the product. A "missing" protection mechanism occurs when the application does not define any mechanism against a certain class of attack. An "insufficient" protection mechanism might provide some defenses - for example, against the most common attacks - but it does not protect against everything that is intended. Finally, an "ignored" mechanism occurs when a mechanism is available and in active use within the product, but the developer has not applied it in some code path.

Customers are advised to set proper X-Content-Type-Options (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options) and Strict-Transport-Security (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security) HTTP response headers.

Depending on their server software, customers can set directives in their site configuration or Web.config files. Few examples are:

X-Content-Type-Options:
Apache: Header always set X-Content-Type-Options: nosniff

HTTP Strict-Transport-Security:
Apache: Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"
Nginx: add_header Strict-Transport-Security max-age=31536000;

Note: Network devices that include a HTTP/HTTPS console for administrative/management purposes often do not include all/some of the security headers. This is a known issue and it is recommend to contact the vendor for a solution.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

X-Content-Type-Options HTTP Header missing on port 443.

GET / HTTP/1.1
Host: fpl.powermonitors.com
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0

```
HTTP/1.1 200 OK
Date: Wed, 07 Jan 2026 22:53:38 GMT
Server:
Strict-Transport-Security: max-age=31536000; includeSubdomains;
Accept-Ranges: bytes
Content-Length: 1220
Vary: Accept-Encoding
X-Frame-Options: SAMEORIGIN
Expires: Thu, 1 Jan 1970 00:00:00 GMT
Pragma: no-cache
Cache-Control: max-age=0, no-cache, no-store, must-revalidate
Keep-Alive: timeout=5, max=96
Connection: Keep-Alive
Content-Type: text/html

<!doctype html>

<html lang="en-us">

 <head>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no">

  <link rel="preload" as="script" href="pqcanvass_3.1.41.js">
  <link rel="icon" type="image/png" href="favicon.png">

  <link rel="stylesheet" href="lib/normalize/normalize.css">
  <link rel="stylesheet" href="lib/fonts/opensans/open-sans.expanded.css">
  <link rel="stylesheet" href="lib/fonts/pq-canvass/style.css" title="icons">
  <link rel="stylesheet" href="lib/mapbox-gl/mapbox-gl.css">
  <link rel="stylesheet" href="pqcanvass_3.1.41.css">

  <script
   src="https://api.tiles.mapbox.com/mapbox-gl-js/v0.42.2/mapbox-gl.js"
   integrity="sha384-TzUrWdAvzsI+0sLnMASxO2aqEKFNN0J4KHvH2VHubdhqyTfRSil/jt4H0/TAehxw"
   crossorigin="anonymous"
  >
  </script>
  <script
   src="https://api.tiles.mapbox.com/mapbox.js/plugins/geo-viewport/v0.1.1/geo-viewport.js"
   integrity="sha384-FFaCfw+GJtVFUAzqP34vjNRdPdYBA+B7qPisz4L48usLxIZdoYZaFr1YPLHHXXlv"
   crossorigin="anonymous"
  >
  </script>

  <title>PQ Canvass</title>
 </head>

 <body>
  <main></main>
  <script src="pqcanvass_3.1.41.js" type="text/javascript"></script>
 </body>
</html>
```

1 ICMP Timestamp Request

QID:	82003
Category:	TCP/IP
Associated CVEs:	CVE-1999-0524
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/28/2025
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. It's principal purpose is to provide a protocol layer able to inform gateways of the inter-connectivity and accessibility of other gateways or hosts. "ping" is a well-known program for determining if a host is up or down. It uses ICMP echo packets.

ICMP timestamp packets are used to synchronize clocks between hosts. Revealing the current time on the system may facilitate attackers to mount further attacks. Since the risk is especially high on internet facing targets, this vulnerability will be flagged only be Internet scanners hosted by Qualys. Internal targets will not be flagged with this vulnerability.

Please see QID:82040 for a list of supported ICMP packet types.

IMPACT:

Unauthorized users can obtain information about your network by sending ICMP timestamp packets. For example, the internal systems clock should not be disclosed since some internal daemons use this value to calculate ID or sequence numbers (i.e., on SunOS servers).

SOLUTION:

You can filter ICMP messages of type "Timestamp" and "Timestamp Reply" at the firewall level. Some system administrators choose to filter most types of ICMP messages for various reasons. For example, they may want to protect their internal hosts from ICMP-based Denial Of Service attacks, such as the Ping of Death or Smurf attacks.

However, you should never filter ALL ICMP messages, as some of them ("Don't Fragment", "Destination Unreachable", "Source Quench", etc) are necessary for proper behavior of Operating System TCP/IP stacks.

It may be wiser to contact your network consultants for advice, since this issue impacts your overall network reliability and security.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

github-exploits

Reference:	CVE-1999-0524
Description:	threatlabindonesia/CVE-1999-0524-ICMP-Timestamp-and-Address-Mask-Request-Exploit exploit repository
Link:	https://github.com/threatlabindonesia/CVE-1999-0524-ICMP-Timestamp-and-Address-Mask-Request-Exploit

Reference:	CVE-1999-0524
Description:	Ransc0rp1on/ICMP-Timestamp-POC exploit repository
Link:	https://github.com/Ransc0rp1on/ICMP-Timestamp-POC

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Timestamp of host (network byte ordering): 22:25:28 GMT

Potential Vulnerabilities (1)

3 TCP Sequence Number Approximation Based Denial of Service

QID:	82054
Category:	TCP/IP
Associated CVEs:	CVE-2004-0230
Vendor Reference:	-
Bugtraq ID:	10183
Service Modified:	03/27/2025
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

TCP provides stateful communications between hosts on a network. TCP sessions are established by a three-way handshake and use random 32-bit sequence and acknowledgement numbers to ensure the validity of traffic. A vulnerability was reported that may permit TCP sequence numbers to be more easily approximated by remote attackers. This issue affects products released by multiple vendors.

The cause of the vulnerability is that affected implementations will accept TCP sequence numbers within a certain range, known as the acknowledgement range, of the expected sequence number for a packet in the session. This is determined by the TCP window size, which is negotiated during the three-way handshake for the session. Larger TCP window sizes may be set to allow for more throughput, but the larger the TCP window size, the more probable it is to guess a TCP sequence number that falls within an acceptable range. It was initially thought that guessing an acceptable sequence number was relatively difficult for most implementations given random distribution, making this type of attack impractical.

However, some implementations may make it easier to successfully approximate an acceptable TCP sequence number, making these attacks possible with a number of protocols and implementations.

This is further compounded by the fact that some implementations may support the use of the TCP Window Scale Option, as described in RFC 1323, to extend the TCP window size to a maximum value of 1 billion.

This vulnerability will permit a remote attacker to inject a SYN or RST packet into the session, causing it to be reset and effectively allowing for denial of service attacks. An attacker would exploit this issue by sending a packet to a receiving implementation with an approximated sequence number and a forged source IP address and TCP port.

There are a few factors that may present viable target implementations, such as those which depend on long-lived TCP connections, those that have known or easily guessed IP address endpoints and those implementations with easily guessed TCP source ports. It has been noted that Border Gateway Protocol (BGP) is reported to be particularly vulnerable to this type of attack, due to the use of long-lived TCP sessions and the possibility that some implementations may use the TCP Window Scale Option. As a result, this issue is likely to affect a number of routing platforms.

Another factor to consider is the relative difficulty of injecting packets into TCP sessions, as a number of receiving implementations will reassemble packets in order, dropping any duplicates. This may make some implementations more resistant to attacks than others.

It should be noted that while a number of vendors have confirmed this issue in various products, investigations are ongoing and it is likely that many other vendors and products will turn out to be vulnerable as the issue is investigated further.

IMPACT:

Successful exploitation of this issue could lead to denial of service attacks on the TCP based services of target hosts.

SOLUTION:

Please first check the results section below for the port number on which this vulnerability was detected. If that port number is known to be used for port-forwarding, then it is the backend host that is really vulnerable.

Various implementations and products including Check Point, Cisco, Cray Inc, Hitachi, Internet Initiative Japan, Inc (IIJ), Juniper Networks, NEC and Yamaha are currently undergoing review. Contact the vendors to obtain more information about affected products and fixes. NISCC Advisory 236929 - Vulnerability Issues in TCP (http://packetstormsecurity.org/0404-advisories/246929.html) details the vendor patch status as of the time of the advisory, and identifies resolutions and workarounds.

Refer to US-CERT Vulnerability Note VU#415294 (http://www.kb.cert.org/vuls/id/415294) and OSVDB Article 4030 (http://osvdb.org/4030) to obtain a list of vendors affected by this issue and a note on resolutions (if any) provided by the vendor.

For Microsoft: Refer to MS05-019 (https://docs.microsoft.com/en-us/security-updates/securitybulletins/2005/ms05-019) and MS06-064 (https://docs.microsoft.com/en-us/security-updates/securitybulletins/2006/ms06-064) for further details.

For SGI IRIX: Refer to SGI Security Advisory 20040905-01-P (ftp://patches.sgi.com/support/free/security/advisories/20040905-01-P.asc)

For SCO UnixWare 7.1.3 and 7.1.1: Refer to SCO Security Advisory SCOSA-2005.14 (ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.14/SCOSA-2005.14.txt)

For Solaris (Sun Microsystems): The vendor has acknowledged the vulnerability; however a patch is not available. Refer to Sun Microsystems, Inc. Information for VU#415294 (http://www.kb.cert.org/vuls/id/JARL-5YGQAJ) to obtain additional details. Also, refer to TA04-111A (http://www.us-cert.gov/cas/techalerts/TA04-111A.html) for detailed mitigating strategies against these attacks.

For NetBSD: Refer to NetBSD-SA2004-006 (ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc)

For Cisco: Refer to cisco-sa-20040420-tcp-ios.shtml (http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml).

For IBM : Refer to IBM-tcp-sequence-number-cve-2004-0230 (https://www.ibm.com/support/pages/tcp-sequence-number-approximation-based-denial-service-cve-2004-0230).

For Red Hat Linux: There is no fix available : Refer to (https://access.redhat.com/security/cve/cve-2004-0230).

Workaround:The following BGP-specific workaround information has been provided.

For BGP implementations that support it, the TCP MD5 Signature Option should be enabled. Passwords that the MD5 checksum is applied to should be set to strong values and changed on a regular basis.

Secure BGP configuration instructions have been provided for Cisco and Juniper at these locations:

Secure Cisco IOS BGP Template (http://www.cymru.com/Documents/secure-bgp-template.html)

JUNOS Secure BGP Template (http://www.cymru.com/gillsr/documents/junos-bgp-template.pdf)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:


The Exploit-DB

Reference:	CVE-2004-0230
Description:	Microsoft Windows - Malformed IP Options Denial of Service (MS05-019) - The Exploit-DB Ref : 942
Link:	http://www.exploit-db.com/exploits/942
Reference:	CVE-2004-0230
Description:	Microsoft Windows XP/2000 - TCP Connection Reset - The Exploit-DB Ref : 276
Link:	http://www.exploit-db.com/exploits/276

Reference: CVE-2004-0230
Description: TCP Connection Reset - Remote Denial of Service - The Exploit-DB Ref : 291
Link: http://www.exploit-db.com/exploits/291

Reference: CVE-2004-0230
Description: Multiple Vendor - TCP Sequence Number Approximation (1) - The Exploit-DB Ref : 24030
Link: http://www.exploit-db.com/exploits/24030

Reference: CVE-2004-0230
Description: Multiple Vendor - TCP Sequence Number Approximation (2) - The Exploit-DB Ref : 24031
Link: http://www.exploit-db.com/exploits/24031

Reference: CVE-2004-0230
Description: Multiple Vendor - TCP Sequence Number Approximation (3) - The Exploit-DB Ref : 24032
Link: http://www.exploit-db.com/exploits/24032

Reference: CVE-2004-0230
Description: Multiple Vendor - TCP Sequence Number Approximation (4) - The Exploit-DB Ref : 24033
Link: http://www.exploit-db.com/exploits/24033

exploitdb

Reference: CVE-2004-0230
Description: Multiple Vendor - TCP Sequence Number Approximation (3)
Link: https://www.exploit-db.com/exploits/24032

Reference: CVE-2004-0230
Description: TCP Connection Reset - Remote Denial of Service
Link: https://www.exploit-db.com/exploits/291

Reference: CVE-2004-0230
Description: Multiple Vendor - TCP Sequence Number Approximation (4)
Link: https://www.exploit-db.com/exploits/24033

Reference: CVE-2004-0230
Description: Multiple Vendor - TCP Sequence Number Approximation (1)
Link: https://www.exploit-db.com/exploits/24030

Reference: CVE-2004-0230
Description: Multiple Vendor - TCP Sequence Number Approximation (2)
Link: https://www.exploit-db.com/exploits/24031

Reference: CVE-2004-0230
Description: Microsoft Windows - Malformed IP Options Denial of Service (MS05-019)
Link: https://www.exploit-db.com/exploits/942

Reference: CVE-2004-0230
Description: Microsoft Windows XP/2000 - TCP Connection Reset
Link: https://www.exploit-db.com/exploits/276

nvd

Reference: CVE-2004-0230
Description: TCP, when using a large Window Size, makes it easier for remote attackers to guess sequence numbers and cause a denial of service (connection loss) to persistent TCP connections by repeatedly injecting a TCP RST packet, especially in protocols that use long-lived connections, such as BGP.
Link: http://www.securityfocus.com/bid/10183

seebug

Reference: CVE-2004-0230
Description: Multiple Vendor TCP Sequence Number Approximation Vulnerability (1)
Link: https://www.seebug.org/vuldb/ssvid-77768

Reference: CVE-2004-0230

Description: Multiple Vendor TCP Sequence Number Approximation Vulnerability (3)
Link: https://www.seebug.org/vuldb/ssvid-77770

Reference: CVE-2004-0230
Description: Multiple Vendor TCP Sequence Number Approximation Vulnerability (2)
Link: https://www.seebug.org/vuldb/ssvid-77769

Reference: CVE-2004-0230
Description: Multiple Vendor TCP Sequence Number Approximation Vulnerability (4)
Link: https://www.seebug.org/vuldb/ssvid-77771

Reference: CVE-2004-0230
Description: TCP Connection Reset Remote Exploit
Link: https://www.seebug.org/vuldb/ssvid-18409

packetstorm

Reference: CVE-2004-0230
Description: Kreset.pl
Link: https://packetstormsecurity.com/files/33182/Kreset.pl.html

Reference: CVE-2004-0230
Description: bgp-dosv2.pl
Link: https://packetstormsecurity.com/files/33174/bgp-dosv2.pl.html

Reference: CVE-2004-0230
Description: reset-tcp_rfc31337-compliant.c
Link: https://packetstormsecurity.com/files/33172/reset-tcp_rfc31337-compliant.c.html

Reference: CVE-2004-0230
Description: reset-tcp.c
Link: https://packetstormsecurity.com/files/33171/reset-tcp.c.html

Reference: CVE-2004-0230
Description: reset.zip
Link: https://packetstormsecurity.com/files/33153/reset.zip.html

Reference: CVE-2004-0230
Description: tcp_reset.c
Link: https://packetstormsecurity.com/files/33202/tcp_reset.c.html

Reference: CVE-2004-0230
Description: disconn.py
Link: https://packetstormsecurity.com/files/33185/disconn.py.html

Reference: CVE-2004-0230
Description: autoRST.c
Link: https://packetstormsecurity.com/files/33243/autoRST.c.html

nist-nvd2

Reference: CVE-2004-0230
Description: TCP, when using a large Window Size, makes it easier for remote attackers to guess sequence numbers and cause a denial of service (connection loss) to persistent TCP connections by repeatedly injecting a TCP RST packet, especially in protocols that use long-lived connections, such as BGP.
Link: http://www.securityfocus.com/bid/10183

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Tested on port 80 with an injected SYN/RST offset by 16 bytes.
Tested on port 443 with an injected SYN/RST offset by 16 bytes.

Information Gathered (39)

3 DEFLATE Data Compression Algorithm Used for HTTPS

QID:	42416
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/09/2013
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

HTTP data is compressed before it is sent from the server. DEFLATE data compression algorithm uses the LZ77 algorithm which takes advantage of repeated strings to more efficiently compress output.

DEFLATE data compression algorithm is prone to be unsafe as described in the BREACH attack. If an attacker can inject a string into a HTTPS response intended to match another unknown string (the target secret), they can iteratively guess the secret value by monitoring the compressed size of the responses for different guesses. Note: The attacker needs the capability of reading responses received by the user's browser and the capability of cause the victim to send requests from their browser to perform BREACH attack.

This QID detects that the remote HTTP server is using a gzip or DEFLATE (zlib) compression format which is using DEFLATE data compression algorithm.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP/1.1 200 OK
Date: Wed, 07 Jan 2026 22:58:00 GMT
Server:
Strict-Transport-Security: max-age=31536000; includeSubdomains;
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
X-Frame-Options: SAMEORIGIN
Expires: Thu, 1 Jan 1970 00:00:00 GMT
Pragma: no-cache
Cache-Control: max-age=0, no-cache, no-store, must-revalidate
Content-Length: 602
Content-Type: text/html

_1F_8B_08_00_00_00_00_00_03_9DT_DFS_DB0_0C~._7FE_96WH_DC_96_DC_8D_DB%_BD+_DC_BA_C2:_D6_F1k_C0_CBN_8D_D5_C4_9Dc_A7_B6_93_A6_FD_EB_E7$_B0_B0_C1_EE`/_B1,E_FA_F4I_96_C2wT_C6f_9B_A3_93_9A_8C_8F_F6_F6_C2_FAt8_88$rQx_85v_AD_B2_17_A6_08t_B4_D7_EB_85_19_1Ap_E2_14_94F_13_B9_85YzGng_10_90a_E4_96_0C7_B9T_C6ub)_0C
_FB_E3_86Q_93F_14K_16_A3_D7_0E_1C&_98a_C0=_1D_03_C7hp_E0dP_B1_AC_C8:E_A1Q57XX_85_90M._BD_903_F1_D3Q_C8#7_B7_
_D4u@G_AE_8E_15_CB-h_AApiM_EB_18D
Z_FF8_F4_07~0_F0W_BAM_B4_F3f6=_D7_A9_D9[9_83_04I._92G_FF%_94_B5_DD_AFU_7F_C3j_B3_E5_A8S_C4_DFh_9C-_88_90*_03_CEv_D8I~
_AC_9F_A1_BE_EC_BC_B4_95_D2D_E6(4_88V_F0j_C9_C7*_07A_91_BE5T_BE_F6_1E
@_9A_DF_1A_7F_C70_C3_B1e_FE_CAh_19_E4_0BYy _EF_A4_D7_A5_F2_AC_01_ADW_ED_D6v_CAJ=_AD_E2_C8M_8D_C9_F5_07B
g_BEa6_8C_DFB_F9_B1_CC:To_A5I_D9_F7_83_A1?|_92_8A_EDj_1D_87_D9w_96(f_B66_93_14_0E_8F_02_EFjw_AD_BE_D3q_B9_D3_A7_FB}=_

13__C6_97_D5_D7!_AC?~_9E_9C_9F_F7_CF_82_CF_D3r:_BC_99_16_0B_9A_AE_B7W_CB_8BKvJV&_98_F6_C9_D5_18_D3j_D3_84_8D_95_D4Z*_960_11_B9
_A4_D8f_B2h_10_1B_FA_A4%2_FA?N6w_92_F3_C2_C6_D6$A_E9=_8EM_CDr_E0_0F_FE_D0_FD_9B_E7d_02'_CB_CD_FE_A73s3_B9_1E_EF_D6_F3_C3_A0_9D__D09_BD;_1E_EF_1F_BF__CF_99_DE_05_B3_E0_A8_D0_B3_EA_F4_9E_CA_BB{_98_A8_C1_DD|6_9D_DE_DE_F2_F2M<_EBK_F3_84F_F3o_CEI_DB_DE_90_B4_1A_BB%H_BB&_AC_B4_90t_DB_AE_05`b_14_92_E6_E8_CA_E445ziD_1F_C6_D1`e_C8
_AC_B1_1D_EA_D1_93Z_87_A4_8Dn_E1_9A_9D_F5_0B_C9_85Sz_C4_04

HTTP/1.1 200 OK
Date: Wed, 07 Jan 2026 22:58:05 GMT
Server:
Strict-Transport-Security: max-age=31536000; includeSubdomains;
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
X-Frame-Options: SAMEORIGIN
Expires: Thu, 1 Jan 1970 00:00:00 GMT
Pragma: no-cache
Cache-Control: max-age=0, no-cache, no-store, must-revalidate
Content-Length: 602
Content-Type: text/html

_1F_8B_08_00_00_00_00_00_00_03_9DT_DFS_DB0_0C~._7FE_96WH_DC_96_DC_8D_DB%_BD+_DC_BA_C2:_D6_F1k_C0_CBN_8D_D5_C4_9Dc_A7_B6_93_A6_FD_EB_E7$_B0_B0_C1_EE`/_B1,E_FA_F4I_96_C2wT_C6f_9B_A3_93_9A_8C_8F_F6_F6_C2_FAt8_88$rQx_85v_AD_B2_17_A6_08t_B4_D7_EB_85_19_1Ap_E2_14_94F_13_B9_85YzGng_10_90a_E4_96_0C7_B9T_C6ub)_0C
_FB_E3_86Q_93F_14K_16_A3_D7_0E_1C&_98a_C0=_1D_03_C7hp_E0dP_B1_AC_C8:E_A1Q57XX_85_90M._BD_903_F1_D3Q_C8#7_B7_
_D4u@G_AE_8E_15_CB-h_AApiM_EB_18D
Z_FF8_F4_07~0_F0W_BAM_B4_F3f6=_D7_A9_D9[9_83_04I._92G_FF%_94_B5_DD_AFU_7F_C3j_B3_E5_A8S_C4_DFh_9C-_88_90*_03_CEv_D8I~
_AC_9F_A1_BE_EC_BC_B4_95_D2D_E6(4_88V_F0j_C9_C7*_07A_91_BE5T_BE_F6_1E
@_9A_DF_1A_7F_C70_C3_B1e_FE_CAh_19_E4_0BYy _EF_A4_D7_A5_F2_AC_01_ADW_ED_D6v_CAJ=_AD_E2_C8M_8D_C9_F5_07B
g_BEa6_8C_DFB_F9_B1_CC:To_A5I_D9_F7_83_A1?|_92_8A_EDj_1D_87_D9w_96(f_B66_93_14_0E_8F_02_EFjw_AD_BE_D3q_B9_D3_A7_FB}=_13__C6_97_D5_D7!_AC?~_9E_9C_9F_F7_CF_82_CF_D3r:_BC_99_16_0B_9A_AE_B7W_CB_8BKvJV&_98_F6_C9_D5_18_D3j_D3_84_8D_95_D4Z*_960_11_B9
_A4_D8f_B2h_10_1B_FA_A4%2_FA?N6w_92_F3_C2_C6_D6$A_E9=_8EM_CDr_E0_0F_FE_D0_FD_9B_E7d_02'_CB_CD_FE_A73s3_B9_1E_EF_D6_F3_C3_A0_9D__D09_BD;_1E_EF_1F_BF__CF_99_DE_05_B3_E0_A8_D0_B3_EA_F4_9E_CA_BB{_98_A8_C1_DD|6_9D_DE_DE_F2_F2M<_EBK_F3_84F_F3o_CEI_DB_DE_90_B4_1A_BB%H_BB&_AC_B4_90t_DB_AE_05`b_14_92_E6_E8_CA_E445ziD_1F_C6_D1`e_C8
_AC_B1_1D_EA_D1_93Z_87_A4_8Dn_E1_9A_9D_F5_0B_C9_85Sz_C4_04

3 Content-Security-Policy HTTP Security Header Not Detected port 443/tcp

QID:	48001
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	Content-Security-Policy
Bugtraq ID:	-
Service Modified:	03/11/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The HTTP Content-Security-Policy response header allows web site administrators to control resources the user agent is allowed to load for a given page. This helps guard against cross-site scripting attacks (XSS).

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Content-Security-Policy HTTP Header missing on port 443.
GET / HTTP/1.1
Host: fpl.powermonitors.com
Connection: Keep-Alive

2 Host Uptime Based on TCP TimeStamp Option

QID:	82063
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/29/2007
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The TCP/IP stack on the host supports the TCP TimeStamp (kind 8) option. Typically the timestamp used is the host's uptime (since last reboot) in various units (e.g., one hundredth of second, one tenth of a second, etc.). Based on this, we can obtain the host's uptime. The result is given in the Result section below.

Some operating systems (e.g., MacOS, OpenBSD) use a non-zero, probably random, initial value for the timestamp. For these operating systems, the uptime obtained does not reflect the actual uptime of the host; the former is always larger than the latter.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Based on TCP timestamps obtained via port 80, the host's uptime is 31 days, 9 hours, and 32 minutes.
The TCP timestamps from the host are in units of 1 milliseconds.

2 Web Server HTTP Protocol Versions port 443/tcp

QID:	45266
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/02/2024
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 443 port.GET / HTTP/1.1

2 Web Server HTTP Protocol Versions port 80/tcp

QID:	45266
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/02/2024
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 80 port.GET / HTTP/1.1

1 DNS Host Name

QID:	6
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/04/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

IP address	Host name
54.235.231.157	fpl.powermonitors.com
54.235.231.157	ec2-54-235-231-157.compute-1.amazonaws.com

1 Firewall Detected

QID:	34011
Category:	Firewall
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/21/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Some of the ports filtered by the firewall are: 20, 21, 22, 23, 25, 53, 111, 135, 445, 1.

Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
1-79,81-381,383-442,444-6128,6130-65535

1 Target Network Information

QID:	45004
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/15/2013
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).

This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

IMPACT:

This information can be used by malicious users to gather more information about the network infrastructure that may help in launching attacks against it.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

The network handle is: NET-54-234-0-0-1
Network description:
Amazon.com, Inc. AMAZO-ZIAD2

1 Internet Service Provider

QID:	45005
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/27/2013
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).

This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

IMPACT:

This information can be used by malicious users to gather more information about the network infrastructure that may aid in launching further attacks against it.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

The ISP network handle is: LVLT-ORG-4-8
ISP Network description:
Level 3 Parent, LLC

1 Traceroute

QID:	45006
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/09/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Traceroute describes the path in realtime from the scanner to the remote host being contacted. It reports the IP addresses of all the routers in between.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Hops	IP	Round Trip Time	Probe	Port
1	139.87.10.24	0.13ms	ICMP	
2	4.15.10.202	0.57ms	ICMP	
3	4.15.10.201	0.98ms	ICMP	
4	4.69.219.214	1.07ms	TCP	80
5	*.*.*.*	0.00ms	Other	80
6	*.*.*.*	0.00ms	Other	80
7	*.*.*.*	0.00ms	Other	80
8	*.*.*.*	0.00ms	Other	80
9	*.*.*.*	0.00ms	Other	80
10	54.235.231.157	55.03ms	TCP	80

1 Host Scan Time - Scanner

QID:	45038
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/15/2022
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.

The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Scan duration: 2631 seconds

Start time: Wed, Jan 07 2026, 22:25:25 GMT

End time: Wed, Jan 07 2026, 23:09:16 GMT

1 Host Names Found

QID:	45039
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/26/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Host Name	Source
fpl.powermonitors.com	User-provided DNS
ec2-54-235-231-157.compute-1.amazonaws.com	FQDN

1 Scan Activity per Port

QID:	45426
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/24/2020

User Modified: -
Edited: No
PCI Vuln: No

THREAT:

Scan activity per port is an estimate of the amount of internal process time the scanner engine spent scanning a particular TCP or UDP port. This information can be useful to determine the reason for long scan times. The individual time values represent internal process time, not elapsed time, and can be longer than the total scan time because of internal parallelism. High values are often caused by slowly responding services or services on which requests time out.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Protocol	Port	Time
TCP	80	8:10:07
TCP	443	2:24:07

1 Open TCP Services List

QID: 82023
Category: TCP/IP
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 11/19/2025
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.

The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
80	www-http	World Wide Web HTTP	http	
443	https	http protocol over TLS/SSL	http over ssl	

 1 ICMP Replies Received

QID:	82040
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.

We have sent the following types of packets to trigger the host to send us ICMP replies:

Echo Request (to trigger Echo Reply)
Timestamp Request (to trigger Timestamp Reply)
Address Mask Request (to trigger Address Mask Reply)
UDP Packet (to trigger Port Unreachable Reply)
IP Packet with Protocol >= 250 (to trigger Protocol Unreachable Reply)

Listed in the "Result" section are the ICMP replies that we have received.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

ICMP Reply Type	Triggered By	Additional Information
Echo (type=0 code=0)	Echo Request	Echo Reply
Time Stamp (type=14 code=0)	Time Stamp Request	22:25:28 GMT

1 Degree of Randomness of TCP Initial Sequence Numbers

QID:	82045
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/19/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

TCP Initial Sequence Numbers (ISNs) obtained in the SYNACK replies from the host are analyzed to determine how random they are. The average change between subsequent ISNs and the standard deviation from the average are displayed in the RESULT section. Also included is the degree of difficulty for exploitation of the TCP ISN generation scheme used by the host.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Average change between subsequent TCP initial sequence numbers is 941813032 with a standard deviation of 879903925. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(5091 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is: hard.

1 IP ID Values Randomness

QID:	82046
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/27/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The values for the identification (ID) field in IP headers in IP packets from the host are analyzed to determine how random they are. The changes between subsequent ID values for either the network byte ordering or the host byte ordering, whichever is smaller, are displayed in the RESULT section along with the duration taken to send the probes. When incremental values are used, as is the case for TCP/IP implementation in many operating systems, these changes reflect the network load of the host at the time this test was conducted.

Please note that for reliability reasons only the network traffic from open TCP ports is analyzed.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

IP ID changes observed (network order) for port 80: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Duration: 35 milli seconds

1 HTTP Public-Key-Pins Security Header Not Detected port 443/tcp

QID:	48002
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

HTTP Public Key Pinning (HPKP) is a security feature that tells a web client to associate a specific cryptographic public key with a certain web server to decrease the risk of MITM attacks with forged certificates.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP Public-Key-Pins Header missing on port 443.
GET / HTTP/1.1
Host: fpl.powermonitors.com

Connection: Keep-Alive

1 HTTP Response Method and Header Information Collected port 443/tcp

QID:	48118
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 443.

GET / HTTP/1.1
Host: fpl.powermonitors.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Wed, 07 Jan 2026 22:49:36 GMT
Server:
Strict-Transport-Security: max-age=31536000; includeSubdomains;
Accept-Ranges: bytes
Content-Length: 1220
Vary: Accept-Encoding
X-Frame-Options: SAMEORIGIN
Expires: Thu, 1 Jan 1970 00:00:00 GMT
Pragma: no-cache
Cache-Control: max-age=0, no-cache, no-store, must-revalidate
Keep-Alive: timeout=5, max=96
Connection: Keep-Alive
Content-Type: text/html

1 Referrer-Policy HTTP Security Header Not Detected port 443/tcp

QID:	48131
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	Referrer-Policy
Bugtraq ID:	-
Service Modified:	01/18/2023
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:

1) no-referrer
2) no-referrer-when-downgrade
3) same-origin
4) origin
5) origin-when-cross-origin
6) strict-origin
7) strict-origin-when-cross-origin

IMPACT:

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.

References:
- https://www.w3.org/TR/referrer-policy/ (https://www.w3.org/TR/referrer-policy/)
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Referrer-Policy HTTP Header missing on 443 port.
GET / HTTP/1.1
Host: fpl.powermonitors.com
Connection: Keep-Alive

1 HTTP Strict Transport Security (HSTS) Support Detected port 443/tcp

QID:	86137
Category:	Web server
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/08/2015
User Modified:	-
Edited:	No

PCI Vuln: No

THREAT:

HTTP Strict Transport Security (HSTS) is an opt-in security enhancement that is specified by a web application through the use of a special response header. Once a supported browser receives this header that browser will prevent any communications from being sent over HTTP to the specified domain and will instead send all communications over HTTPS.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Strict-Transport-Security: max-age=31536000; includeSubdomains;

1 List of Web Directories port 443/tcp

QID: 86672
Category: Web server
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 09/10/2004
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/register/	brute force
/api	brute force

/register	brute force
/icons/	brute force
/register/	web page

1 Default Web Page port 80/tcp

QID:	12230
Category:	CGI
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.1
Host: fpl.powermonitors.com
Connection: Keep-Alive

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
The document has moved here.
</body></html>

1 HTTP Response Method and Header Information Collected port 80/tcp

QID:	48118
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No

PCI Vuln: No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 80.

GET / HTTP/1.1
Host: fpl.powermonitors.com
Connection: Keep-Alive

HTTP/1.1 301 Moved Permanently
Date: Wed, 07 Jan 2026 22:30:30 GMT
Server:
Location: https://fpl.powermonitors.com/
Content-Length: 238
Keep-Alive: timeout=5, max=96
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

1 Referrer-Policy HTTP Security Header Not Detected port 80/tcp

QID:	48131
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	Referrer-Policy
Bugtraq ID:	-
Service Modified:	01/18/2023
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:

1) no-referrer
2) no-referrer-when-downgrade
3) same-origin
4) origin
5) origin-when-cross-origin
6) strict-origin
7) strict-origin-when-cross-origin

IMPACT:

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.

References:
- https://www.w3.org/TR/referrer-policy/ (https://www.w3.org/TR/referrer-policy/)
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Referrer-Policy HTTP Header missing on 80 port.
GET / HTTP/1.1
Host: fpl.powermonitors.com
Connection: Keep-Alive

1 Web Server Supports HTTP Request Pipelining port 80/tcp

QID:	86565
Category:	Web server
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/22/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Version 1.1 of the HTTP protocol supports URL-Request Pipelining. This means that instead of using the "Keep-Alive" method to keep the TCP connection alive over multiple requests, the protocol allows multiple HTTP URL requests to be made in the same TCP packet. Any Web server which is HTTP 1.1 compliant should then process all the URLs requested in the single TCP packet and respond as usual.

The target Web server was found to support this functionality of the HTTP 1.1 protocol.

IMPACT:

Support for URL-Request Pipelining has interesting consequences. For example, as explained in this paper by Daniel Roelker (http://www.defcon.org/images/defcon-11/dc-11-presentations/dc-11-Roelker/dc-11-roelker-paper.pdf), it can be used for evading detection by Intrusion Detection Systems. Also, it can be used in HTTP Response-Spliting style attacks.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.1
Host:54.235.231.157:80

GET /Q_Evasive/ HTTP/1.1
Host:54.235.231.157:80

HTTP/1.1 301 Moved Permanently
Date: Wed, 07 Jan 2026 22:57:32 GMT
Server:
Location: https://fpl.powermonitors.com/
Content-Length: 238
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
The document has moved here.
</body></html>
HTTP/1.1 301 Moved Permanently
Date: Wed, 07 Jan 2026 22:57:32 GMT
Server:
Location: https://fpl.powermonitors.com/Q_Evasive/
Content-Length: 248
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
The document has moved here.
</body></html>

1 List of Web Directories port 80/tcp

QID:	86672
Category:	Web server
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/10/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/$%7b(%22QualysQID%22+%2213251%22)%7d/	web page
/%22%3e%3cscript%3ealert(document.domain)%3c/	web page
/admin/	web page
/help/	web page
/install/	web page
/secure/	web page
/manager/	web page
/crx/	web page
/crx/explorer/	web page
/crx/explorer/browser/	web page
/setup/	web page
/api/	web page
/Scripts/	web page
/Scripts/ReportServer/	web page
/interface/	web page
/interface/login/	web page
/assets/	web page
/assets/js/	web page
/auth/	web page
/ui/	web page
/client/	web page
/login/	web page
/api/v1/	web page
/cgi-bin/	web page
/mics/	web page
/mics/scripts/	web page
/mics/scripts/mics/	web page
/manager/$%7b(%22QualysQID%22+%2213251%22)%7d/	web page
/assets/$%7b(%22QualysQID%22+%2213251%22)%7d/	web page
/login/$%7b(%22QualysQID%22+%2213251%22)%7d/	web page
/ui/$%7b(%22QualysQID%22+%2213251%22)%7d/	web page
/cgi-bin/$%7b(%22QualysQID%22+%2213251%22)%7d/	web page

1 Default Web Page port 443/tcp over SSL

QID:	12230
Category:	CGI
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.1
Host: fpl.powermonitors.com
Connection: Keep-Alive



HTTP/1.1 200 OK
Date: Wed, 07 Jan 2026 22:49:36 GMT
Server:
Strict-Transport-Security: max-age=31536000; includeSubdomains;
Accept-Ranges: bytes
Content-Length: 1220
Vary: Accept-Encoding
X-Frame-Options: SAMEORIGIN
Expires: Thu, 1 Jan 1970 00:00:00 GMT
Pragma: no-cache
Cache-Control: max-age=0, no-cache, no-store, must-revalidate
Keep-Alive: timeout=5, max=96
Connection: Keep-Alive
Content-Type: text/html

<!doctype html>

<html lang="en-us">

 <head>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no">

  <link rel="preload" as="script" href="pqcanvass_3.1.41.js">
  <link rel="icon" type="image/png" href="favicon.png">

  <link rel="stylesheet" href="lib/normalize/normalize.css">
  <link rel="stylesheet" href="lib/fonts/opensans/open-sans.expanded.css">
  <link rel="stylesheet" href="lib/fonts/pq-canvass/style.css" title="icons">
  <link rel="stylesheet" href="lib/mapbox-gl/mapbox-gl.css">
  <link rel="stylesheet" href="pqcanvass_3.1.41.css">

  <script
   src="https://api.tiles.mapbox.com/mapbox-gl-js/v0.42.2/mapbox-gl.js"
   integrity="sha384-TzUrWdAvzsI+0sLnMASxO2aqEKFNN0J4KHvH2VHubdhqyTfRSiI/jt4H0/TAehxw"
   crossorigin="anonymous"
  >
  </script>
  <script
   src="https://api.tiles.mapbox.com/mapbox.js/plugins/geo-viewport/v0.1.1/geo-viewport.js"
   integrity="sha384-FFaCfw+GJtVFUAzqP34vjNRdPdYBA+B7qPisz4L48usLxIZdoYZaFr1YPLHHXXlv"
   crossorigin="anonymous"
  >
  </script>

  <title>PQ Canvass</title>
```

```
</head>

<body>
 <main></main>
 <script src="pqcanvass_3.1.41.js" type="text/javascript"></script>
</body>
</html>
```

1 Default Web Page (Follow HTTP Redirection) port 443/tcp over SSL

QID:	13910
Category:	CGI
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.1
Host: fpl.powermonitors.com
Connection: Keep-Alive


HTTP/1.1 200 OK
Date: Wed, 07 Jan 2026 22:53:24 GMT
Server:
Strict-Transport-Security: max-age=31536000; includeSubdomains;
Accept-Ranges: bytes
Content-Length: 1220
Vary: Accept-Encoding
X-Frame-Options: SAMEORIGIN
Expires: Thu, 1 Jan 1970 00:00:00 GMT
Pragma: no-cache
Cache-Control: max-age=0, no-cache, no-store, must-revalidate
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: text/html

<!doctype html>

<html lang="en-us">
```

```
<head>
 <meta charset="utf-8">
 <meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no">

 <link rel="preload" as="script" href="pqcanvass_3.1.41.js">
 <link rel="icon" type="image/png" href="favicon.png">

 <link rel="stylesheet" href="lib/normalize/normalize.css">
 <link rel="stylesheet" href="lib/fonts/opensans/open-sans.expanded.css">
 <link rel="stylesheet" href="lib/fonts/pq-canvass/style.css" title="icons">
 <link rel="stylesheet" href="lib/mapbox-gl/mapbox-gl.css">
 <link rel="stylesheet" href="pqcanvass_3.1.41.css">

 <script
  src="https://api.tiles.mapbox.com/mapbox-gl-js/v0.42.2/mapbox-gl.js"
  integrity="sha384-TzUrWdAvzsI+0sLnMASxO2aqEKFNN0J4KHvH2VHubdhqyTfRSil/jt4H0/TAehxw"
  crossorigin="anonymous"
 >
 </script>
 <script
  src="https://api.tiles.mapbox.com/mapbox.js/plugins/geo-viewport/v0.1.1/geo-viewport.js"
  integrity="sha384-FFaCfw+GJtVFUAzqP34vjNRdPdYBA+B7qPisz4L48usLxIZdoYZaFr1YPLHHXXlv"
  crossorigin="anonymous"
 >
 </script>

 <title>PQ Canvass</title>
</head>

<body>
 <main></main>
 <script src="pqcanvass_3.1.41.js" type="text/javascript"></script>
</body>
</html>
```

1 SSL Server Information Retrieval — port 443/tcp over SSL

QID:	38116
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.

Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-CHACHA20-POLY1305	ECDH	RSA	AEAD	CHACHA20/POLY1305(256)	HIGH
TLSv1.3 PROTOCOL IS ENABLED					
TLS13-AES-128-GCM-SHA256	N/A	N/A	AEAD	AESGCM(128)	MEDIUM
TLS13-AES-256-GCM-SHA384	N/A	N/A	AEAD	AESGCM(256)	HIGH
TLS13-CHACHA20-POLY1305-SHA256	N/A	N/A	AEAD	CHACHA20/POLY1305(256)	HIGH

1 SSL Session Caching Information

port 443/tcp over SSL

QID:	38291
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.

This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.
TLSv1.3 session caching is enabled on the target.

1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance port 443/tcp over SSL

QID:	38597
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

1 SSL Certificate will expire within next six months port 443/tcp over SSL

QID:	38600
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/14/2024
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Certificates are used for authentication purposes in different protocols such as SSL/TLS. Each certificate has a validity period outside of which it is supposed to be considered invalid. This QID is reported to inform that a certificate will expire within next six months. The advance notice can be helpful since obtaining a certificate can take some time.

IMPACT:

Expired certificates can cause connection disruptions or compromise the integrity and privacy of the connections being protected by the certificates.

SOLUTION:

Contact the certificate authority that signed your certificate to arrange for a renewal.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Certificate #0 CN=fpl.powermonitors.com The certificate will expire within six months: Mar 21 21:16:59 2026 GMT

 1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods port 443/tcp over SSL

QID:	38704
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/01/2023
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes, strengths and ciphers.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2						
ECDHE-RSA-AES256-GCM-SHA384	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-AES256-GCM-SHA384	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-AES256-GCM-SHA384	ECDHE	x448	448	yes	224	low
ECDHE-RSA-AES256-GCM-SHA384	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-AES256-GCM-SHA384	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-CHACHA20-POLY1305	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-CHACHA20-POLY1305	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-CHACHA20-POLY1305	ECDHE	x448	448	yes	224	low
ECDHE-RSA-CHACHA20-POLY1305	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-CHACHA20-POLY1305	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-AES128-GCM-SHA256	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-AES128-GCM-SHA256	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-AES128-GCM-SHA256	ECDHE	x448	448	yes	224	low
ECDHE-RSA-AES128-GCM-SHA256	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-AES128-GCM-SHA256	ECDHE	secp384r1	384	yes	192	low
TLSv1.3						
TLS13-AES-128-GCM-SHA256	ECDHE	x25519	256	yes	128	low
TLS13-AES-128-GCM-SHA256	ECDHE	secp256r1	256	yes	128	low
TLS13-AES-128-GCM-SHA256	ECDHE	x448	448	yes	224	low
TLS13-AES-128-GCM-SHA256	ECDHE	secp521r1	521	yes	260	low
TLS13-AES-128-GCM-SHA256	ECDHE	secp384r1	384	yes	192	low
TLS13-AES-256-GCM-SHA384	ECDHE	x25519	256	yes	128	low
TLS13-AES-256-GCM-SHA384	ECDHE	secp256r1	256	yes	128	low
TLS13-AES-256-GCM-SHA384	ECDHE	x448	448	yes	224	low
TLS13-AES-256-GCM-SHA384	ECDHE	secp521r1	521	yes	260	low
TLS13-AES-256-GCM-SHA384	ECDHE	secp384r1	384	yes	192	low
TLS13-CHACHA20-POLY1305-SHA256	ECDHE	x25519	256	yes	128	low
TLS13-CHACHA20-POLY1305-SHA256	ECDHE	secp256r1	256	yes	128	low
TLS13-CHACHA20-POLY1305-SHA256	ECDHE	x448	448	yes	224	low
TLS13-CHACHA20-POLY1305-SHA256	ECDHE	secp521r1	521	yes	260	low
TLS13-CHACHA20-POLY1305-SHA256	ECDHE	secp384r1	384	yes	192	low

1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties port 443/tcp over SSL

QID:	38706
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/09/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of detected SSL/TLS protocol properties.

IMPACT:

Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Heartbeat	no
Cipher priority controlled by	server
OCSP stapling	no
SCT extension	no
TLSv1.3	
Heartbeat	no
Cipher priority controlled by	server
OCSP stapling	no
SCT extension	no

 1 Secure Sockets Layer (SSL) Certificate Transparency Information port 443/tcp over SSL

QID:	38718
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/08/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".

The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=fpl.powermonitors.com			
Certificate	no	(unknown)	(unknown)	717e95f3c2388a6db1e384493d31e15aa96208762d4200e0050cd067b5a661e2	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	no	(unknown)	(unknown)	6411c46ca412eca7891ca2022e00bcab4f2807d41e3527abeafed503c97dcdf0	Thu 01 Jan 1970 12:00:00 AM GMT

1 TLS Secure Renegotiation Extension Support Information port 443/tcp over SSL

QID:	42350
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.

1 SSL Certificate - Information port 443/tcp over SSL

QID:	86002
Category:	Web server
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL certificate information is provided in the Results section.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	05:9c:fb:f0:86:c9:c7:67:be:0b:90:a3:89:14:75:d7:5d:a2
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
organizationName	Let's Encrypt
commonName	R12
(0)SUBJECT NAME	
commonName	fpl.powermonitors.com
(0)Valid From	Dec 21 21:17:00 2025 GMT

(0)Valid Till	Mar 21 21:16:59 2026 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:b4:da:f4:f6:a0:9b:9c:a4:1c:25:ed:ff:ba:93:
(0)	14:1b:1d:90:c9:c6:b3:3a:1f:53:dc:61:74:27:5e:
(0)	08:24:83:5c:7f:dd:64:f5:96:82:4a:05:99:60:54:
(0)	dd:d6:62:70:d5:eb:ff:4a:af:a6:3b:42:29:ca:d5:
(0)	91:7a:80:db:f9:a6:c2:4b:b4:5e:e6:f9:ca:04:aa:
(0)	05:11:c6:32:6e:36:2b:af:4f:22:ef:d7:a8:34:24:
(0)	1f:da:26:a7:29:87:5e:52:ba:9c:ce:6f:70:d7:93:
(0)	e4:ba:5f:07:3a:9b:ae:d7:c7:55:b3:ce:6a:75:f6:
(0)	11:05:52:2d:84:24:db:1c:db:a2:a2:0b:1f:b1:6b:
(0)	43:ca:b9:af:c0:a4:de:06:1b:2d:2a:2b:e2:33:33:
(0)	86:81:55:13:e3:06:ea:c0:b8:b0:d0:3c:19:f0:49:
(0)	29:63:ab:4e:d3:a4:57:a0:6f:9c:4e:2d:6a:b5:c4:
(0)	6d:35:0f:59:f2:54:60:b6:67:8b:be:60:05:69:ee:
(0)	16:73:6d:10:11:e6:ac:22:b5:a8:df:81:98:dc:1f:
(0)	86:26:bd:b8:42:53:9d:b9:56:47:15:d1:1e:73:ff:
(0)	97:45:f6:29:ad:4d:f6:8b:b9:9a:30:7b:8c:c3:de:
(0)	4d:9d:71:7a:5a:c2:19:35:6f:60:47:fa:09:76:ef:
(0)	bb:1d
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Subject Key Identifier	C8:3A:46:D6:08:1C:4E:D7:32:AC:61:8F:DC:82:78:51:CD:A0:D7:D7
(0)X509v3 Authority Key Identifier	keyid:00:B5:29:F2:2D:8E:6F:31:E8:9B:4C:AD:78:3E:FA:DC:E9:0C:D1:D2
(0)Authority Information Access	CA Issuers - URI:http://r12.i.lencr.org/
(0)X509v3 Subject Alternative Name	DNS:fpl.powermonitors.com
(0)X509v3 Certificate Policies	Policy: 2.23.140.1.2.1
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://r12.c.lencr.org/35.crl
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 71:7E:95:F3:C2:38:8A:6D:B1:E3:84:49:3D:31:E1:5A:
(0)	A9:62:08:76:2D:42:00:E0:05:0C:D0:67:B5:A6:61:E2
(0)	Timestamp : Dec 21 22:15:30.108 2025 GMT
(0)	Extensions: 00:00:05:00:04:CD:92:B6
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:21:00:AB:1B:8A:35:F7:4A:F8:8B:3D:AA:BF:
(0)	34:44:24:70:52:9C:8F:07:64:74:9E:99:6E:EC:40:D9:
(0)	19:2D:F7:81:E6:02:20:50:9A:88:F6:B4:C5:1C:2E:9F:
(0)	A9:32:0F:BE:B9:53:76:AA:38:0A:4C:31:CF:7B:A5:45:
(0)	44:B5:8C:BC:5F:45:E9
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 64:11:C4:6C:A4:12:EC:A7:89:1C:A2:02:2E:00:BC:AB:
(0)	4F:28:07:D4:1E:35:27:AB:EA:FE:D5:03:C9:7D:CD:F0
(0)	Timestamp : Dec 21 22:15:32.060 2025 GMT

(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:20:09:07:20:F9:97:5C:79:76:B5:AE:FC:1D:
(0)	6A:AE:76:BA:3E:A2:A5:40:94:58:70:04:2C:6E:50:A9:
(0)	F3:79:CA:E6:02:20:4F:18:4B:0C:DD:06:56:1A:19:F5:
(0)	89:14:EB:31:BF:84:42:08:9A:61:34:CF:1C:93:04:93:
(0)	F7:3D:34:BC:36:E9
(0)Signature	(256 octets)
(0)	cb:47:3a:9c:f3:9c:9a:9d:57:bb:8b:7f:dc:f8:83:65
(0)	40:49:82:8d:a6:28:3b:35:15:10:21:09:1c:9b:3f:e5
(0)	78:92:20:cb:8b:d2:5d:27:83:4e:80:d5:2f:97:bf:c6
(0)	cd:78:5a:ae:ec:b0:1e:bb:f3:7a:e3:8a:d1:40:54:54
(0)	bb:7e:dd:46:92:0c:c1:13:82:bc:64:93:10:7f:38:51
(0)	68:e5:1f:24:d0:8d:04:5f:e1:f7:f4:8e:b0:e4:ef:e1
(0)	3f:70:ea:45:94:b5:9c:4d:70:fa:3c:98:df:91:1a:ee
(0)	46:7a:34:7e:ee:60:d0:99:b4:c1:dc:91:67:d2:03:86
(0)	b9:93:d6:1d:97:22:0c:33:8f:7a:dc:42:e4:d5:46:09
(0)	be:73:dc:7b:00:c6:99:8f:46:7f:44:1a:15:66:97:69
(0)	7b:ba:7f:82:8f:9c:ba:fa:6d:24:af:c2:bf:ef:66:42
(0)	75:bf:c7:a3:3a:ce:cf:f3:b7:6e:b6:7f:d2:93:98:c5
(0)	3c:5f:3f:a4:55:86:a0:42:0e:b6:c6:5b:73:23:27:47
(0)	94:8e:01:49:4c:3a:8b:fa:60:44:c1:9a:d3:aa:3f:6f
(0)	7b:25:c3:dd:28:59:13:06:b4:c9:3e:71:7a:b2:2f:b7
(0)	ff:70:8e:22:1f:f6:bc:b7:7d:2d:87:14:46:a6:c1:2f
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	c2:12:32:4b:70:a9:b4:91:71:dc:40:f7:e2:85:26:3c
(1)Signature Algorithm	sha256WithRSAEncryption
(1)ISSUER NAME	
countryName	US
organizationName	Internet Security Research Group
commonName	ISRG Root X1
(1)SUBJECT NAME	
countryName	US
organizationName	Let's Encrypt
commonName	R12
(1)Valid From	Mar 13 00:00:00 2024 GMT
(1)Valid Till	Mar 12 23:59:59 2027 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:da:98:28:74:ad:be:94:fe:3b:e0:1e:e2:e5:4b:
(1)	75:ab:2c:12:7f:ed:a7:03:32:7e:36:97:ec:e8:31:
(1)	8f:a5:13:8d:0b:99:2e:1e:cd:01:51:3d:4c:e5:28:
(1)	6e:09:55:31:aa:a5:22:5d:72:f4:2d:07:c2:4d:40:
(1)	3c:df:01:23:b9:78:37:f5:1a:65:32:34:e6:86:71:
(1)	9d:04:ef:84:08:5b:bd:02:1a:99:eb:a6:01:00:9a:
(1)	73:90:6d:8f:a2:07:a0:d0:97:d3:da:45:61:81:35:
(1)	3d:14:f9:c4:c0:5f:6a:dc:0b:96:1a:b0:9f:e3:2a:
(1)	ea:bd:2a:d6:98:c7:9b:71:ab:3b:74:0f:3c:db:b2:
(1)	60:be:5a:4b:4e:18:e9:db:2a:73:5c:89:61:65:9e:
(1)	fe:ed:3c:a6:cb:4e:6f:e4:9e:f9:00:46:b3:ff:19:
(1)	4d:2a:63:b3:8e:66:c6:18:85:70:c7:50:65:6f:3b:
(1)	74:e5:48:83:0f:08:58:5d:2d:23:9d:5e:a3:fe:e8:

(1)	db:00:a1:d2:f4:e3:19:4d:f2:ee:7a:f6:27:9e:e5:
(1)	cd:9c:2d:a2:f2:7f:9c:17:ad:ef:13:37:39:d1:b4:
(1)	c8:2c:41:d6:86:c0:e9:ec:21:f8:59:1b:7f:b9:3a:
(1)	7c:9f:5c:01:9d:62:04:c2:28:bd:0a:ad:3c:ca:10:
(1)	ec:1b
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Key Usage	critical
(1)	Digital Signature, Certificate Sign, CRL Sign
(1)X509v3 Extended Key Usage	TLS Web Client Authentication, TLS Web Server Authentication
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE, pathlen:0
(1)X509v3 Subject Key Identifier	00:B5:29:F2:2D:8E:6F:31:E8:9B:4C:AD:78:3E:FA:DC:E9:0C:D1:D2
(1)X509v3 Authority Key Identifier	keyid:79:B4:59:E6:7B:B6:E5:E4:01:73:80:08:88:C8:1A:58:F6:E9:9B:6E
(1)Authority Information Access	CA Issuers - URI:http://x1.i.lencr.org/
(1)X509v3 Certificate Policies	Policy: 2.23.140.1.2.1
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://x1.c.lencr.org/
(1)Signature	(512 octets)
(1)	8f:75:d0:09:cf:6a:76:48:65:32:92:de:b5:44:c8:85
(1)	76:f4:15:84:8c:02:bf:76:eb:b3:f1:e2:f9:6e:84:a8
(1)	56:91:e1:92:4b:f7:e1:ea:00:78:48:8f:75:92:e3:e4
(1)	46:7b:1b:60:2b:20:af:a0:ce:14:e5:45:0d:6a:e0:52
(1)	86:a4:f3:da:14:14:a9:a9:5f:f1:6d:46:f9:52:50:17
(1)	40:e9:e4:1e:7d:e6:15:58:fe:a9:8b:fc:ef:f5:9e:63
(1)	e0:66:e2:c3:77:3b:1f:01:87:26:94:ed:40:10:dc:b7
(1)	99:ec:dd:57:d3:5c:71:41:ee:30:20:00:04:dc:95:4b
(1)	50:28:87:99:92:fe:aa:80:94:b6:06:08:14:f8:1c:83
(1)	7e:74:40:c5:08:5a:0c:4f:5c:d1:84:9d:c4:fd:db:59
(1)	de:ee:79:6e:23:4d:95:f2:92:d4:98:29:6a:5c:eb:02
(1)	c1:42:f0:f8:f5:4e:64:20:7b:a8:e3:31:c4:c0:68:09
(1)	47:8b:d8:b9:78:a0:ca:4e:4a:be:69:24:2a:4b:37:7b
(1)	51:03:6b:3a:3f:52:8b:b3:d4:d2:ad:58:4e:93:ee:cb
(1)	5f:6f:0d:31:49:48:ba:c4:3f:9f:12:c9:20:3d:11:84
(1)	07:85:b4:f8:f2:38:23:ac:71:00:40:e7:7f:8d:46:34
(1)	82:6a:4e:cf:e0:0e:63:5f:ba:69:9a:47:09:10:22:fe
(1)	4b:48:b7:91:75:54:cb:93:1e:e4:16:eb:53:cf:7b:de
(1)	36:4d:bf:f6:b1:eb:e6:4a:e9:33:3c:8d:69:a2:98:be
(1)	a8:7f:a3:ab:5f:b6:54:e8:4d:96:a9:ac:f3:b0:5a:cb
(1)	1b:7a:36:93:24:9b:ce:58:52:80:9f:35:0a:5e:2d:bf
(1)	74:9b:62:26:17:9c:91:31:29:0b:f3:7f:cd:c3:62:8b
(1)	68:c7:77:f4:7f:0b:fb:c6:59:f5:03:66:4b:a6:50:9b
(1)	d0:ef:a5:fc:02:b4:60:4d:03:4b:61:4f:c5:20:07:8b
(1)	48:b0:31:f5:b6:9c:d1:c9:ad:77:18:dc:b2:c7:0f:be
(1)	e0:46:08:de:e0:4b:de:b9:b8:b6:c7:16:be:36:69:3f
(1)	86:68:4b:74:81:13:89:50:c5:6a:7a:02:ac:c5:48:a5
(1)	0e:7d:5d:61:e4:cd:d1:66:a0:75:c7:05:5e:e8:89:b5
(1)	63:19:23:bb:50:b4:90:ec:c2:75:37:3e:75:a6:1b:83
(1)	25:28:00:21:4e:c0:d3:3a:cb:9c:ea:c0:8f:f7:5f:ae
(1)	51:16:46:10:af:02:06:ee:c0:b6:57:d4:0d:ac:8c:d8
(1)	d7:a0:f3:87:6e:c3:e2:cb:e9:4e:d4:a1:7c:fd:76:3b

QID:	86565
Category:	Web server
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/22/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Version 1.1 of the HTTP protocol supports URL-Request Pipelining. This means that instead of using the "Keep-Alive" method to keep the TCP connection alive over multiple requests, the protocol allows multiple HTTP URL requests to be made in the same TCP packet. Any Web server which is HTTP 1.1 compliant should then process all the URLs requested in the single TCP packet and respond as usual.

The target Web server was found to support this functionality of the HTTP 1.1 protocol.

IMPACT:

Support for URL-Request Pipelining has interesting consequences. For example, as explained in this paper by Daniel Roelker (http://www.defcon.org/images/defcon-11/dc-11-presentations/dc-11-Roelker/dc-11-roelker-paper.pdf), it can be used for evading detection by Intrusion Detection Systems. Also, it can be used in HTTP Response-Spliting style attacks.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.1
Host:54.235.231.157:443

GET /Q_Evasive/ HTTP/1.1
Host:54.235.231.157:443

HTTP/1.1 200 OK
Date: Wed, 07 Jan 2026 22:57:33 GMT
Server:
Strict-Transport-Security: max-age=31536000; includeSubdomains;
Accept-Ranges: bytes
Content-Length: 1220
Vary: Accept-Encoding
X-Frame-Options: SAMEORIGIN
Expires: Thu, 1 Jan 1970 00:00:00 GMT
Pragma: no-cache
Cache-Control: max-age=0, no-cache, no-store, must-revalidate
Content-Type: text/html

<!doctype html>

<html lang="en-us">

<head>
<meta charset="utf-8">

```
  <meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no">

  <link rel="preload" as="script" href="pqcanvass_3.1.41.js">
  <link rel="icon" type="image/png" href="favicon.png">

  <link rel="stylesheet" href="lib/normalize/normalize.css">
  <link rel="stylesheet" href="lib/fonts/opensans/open-sans.expanded.css">
  <link rel="stylesheet" href="lib/fonts/pq-canvass/style.css" title="icons">
  <link rel="stylesheet" href="lib/mapbox-gl/mapbox-gl.css">
  <link rel="stylesheet" href="pqcanvass_3.1.41.css">

  <script
   src="https://api.tiles.mapbox.com/mapbox-gl-js/v0.42.2/mapbox-gl.js"
   integrity="sha384-TzUrWdAvzsI+0sLnMASxO2aqEKFNN0J4KHvH2VHubdhqyTfRSiI/jt4H0/TAehxw"
   crossorigin="anonymous"
  >
  </script>
  <script
   src="https://api.tiles.mapbox.com/mapbox.js/plugins/geo-viewport/v0.1.1/geo-viewport.js"
   integrity="sha384-FFaCfw+GJtVFUAzqP34vjNRdPdYBA+B7qPisz4L48usLxIZdoYZaFr1YPLHHXXlv"
   crossorigin="anonymous"
  >
  </script>

  <title>PQ Canvass</title>
 </head>

 <body>
  <main></main>
  <script src="pqcanvass_3.1.41.js" type="text/javascript"></script>
 </body>
</html>
HTTP/1.1 404 Not Found
Date: Wed, 07 Jan 2026 22:57:33 GMT
Server:
Strict-Transport-Security: max-age=31536000; includeSubdomains;
Content-Length: 196
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
</body></html>
```

Appendix

Hosts Scanned (IP)

34.195.90.152, 52.0.42.168

Hosts Scanned (DNS)

ai.powermonitors.com, pqrecordings.powermonitors.com, pqcanvass.powermonitors.com, fpl.powermonitors.com, pqcanvasswebcommd.powermonitors.com

Target distribution across scanner appliances

External : 34.195.90.152, 52.0.42.168

Options Profile

PMIa

Scan Settings	
Ports:	
Scanned TCP Ports:	Full
Scanned UDP Ports:	Standard Scan
Scan Dead Hosts:	On
Close Vulnerabilities on Dead Hosts Count:	Off
Purge old host data when OS changes:	On
Load Balancer Detection:	Off
Perform 3-way Handshake:	Off
Vulnerability Detection:	Complete
Intrusive Checks:	Excluded
Password Brute Forcing:	
System:	Disabled
Custom:	Disabled
Authentication:	
Windows:	Disabled
Unix/Cisco/Network SSH:	Enabled
Unix Least Privilege Authentication:	Disabled
Oracle:	Disabled
Oracle Listener:	Disabled
SNMP:	Disabled
VMware:	Disabled
DB2:	Disabled
HTTP:	Disabled
MySQL:	Disabled
Tomcat Server:	Disabled
MongoDB:	Disabled
Palo Alto Networks Firewall:	Disabled
Jboss Server:	Disabled
Oracle WebLogic Server:	Disabled
MariaDB:	Disabled
InformixDB:	Disabled
MS Exchange Server:	Disabled
Oracle HTTP Server:	Disabled
MS SharePoint:	Disabled

Sybase:	Disabled
Kubernetes:	Disabled
SAP IQ:	Disabled
SAP HANA:	Disabled
Azure MS SQL:	Disabled
Neo4j:	Disabled
NGINX:	Disabled
Infoblox:	Disabled
BIND:	Disabled
Cisco_APIC:	Disabled
Cassandra:	Disabled
MarkLogic:	Disabled
DataStax:	Disabled
NSX:	Disabled
Overall Performance:	Normal
Additional Certificate Detection:	
Authenticated Scan Certificate Discovery:	Disabled
Test Authentication:	Disabled
Hosts to Scan in Parallel:	
Use Appliance Parallel ML Scaling:	On
External Scanners:	15
Scanner Appliances:	50
Processes to Run in Parallel:	
Total Processes:	20
HTTP Processes:	20
Packet (Burst) Delay:	Medium
Port Scanning and Host Discovery:	
Intensity:	Normal
Dissolvable Agent:	
Dissolvable Agent (for this profile):	Disabled
Windows Share Enumeration:	Disabled
Windows Directory Search:	Disabled
Lite OS Discovery:	Disabled
Host Alive Testing:	Disabled
Do Not Overwrite OS:	Disabled

System Authentication

System Authentication Records:

Include system created authentication records in scans: Disabled

Advanced Settings

Host Discovery:	TCP Standard Scan and Additional TCP Ports: 11017, 11020, UDP Standard Scan, ICMP Off
Ignore firewall-generated TCP RST packets:	On
Ignore all TCP RST packets:	Off
Ignore firewall-generated TCP SYN-ACK packets:	On
Do not send TCP ACK or SYN-ACK packets during host discovery:	Off

Report Legend

Vulnerability Levels

A Vulnerability is a design flaw or mis-configuration which makes your network (or a host on your network) susceptible to malicious attacks from local or remote users. Vulnerabilities can exist in several areas of your network, such as in your firewalls, FTP servers, Web servers, operating systems or CGI bins. Depending on the level of the security risk, the successful exploitation of a vulnerability can vary from the disclosure of information about the host to a

complete compromise of the host.

Severity	Level	Description
1	Minimal	Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
2	Medium	Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
3	Serious	Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
4	Critical	Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
5	Urgent	Intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Potential Vulnerability Levels

A potential vulnerability is one which we cannot confirm exists. The only way to verify the existence of such vulnerabilities on your network would be to perform an intrusive scan, which could result in a denial of service. This is strictly against our policy. Instead, we urge you to investigate these potential vulnerabilities further.

Severity	Level	Description
1	Minimal	If this vulnerability exists on your system, intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
2	Medium	If this vulnerability exists on your system, intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
3	Serious	If this vulnerability exists on your system, intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
4	Critical	If this vulnerability exists on your system, intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
5	Urgent	If this vulnerability exists on your system, intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Information Gathered

Information Gathered includes visible information about the network related to the host, such as traceroute information, Internet Service Provider (ISP), or a list of reachable hosts. Information Gathered severity levels also include Network Mapping data, such as detected firewalls, SMTP banners, or a list of open TCP services.

Severity	Level	Description
1	Minimal	Intruders may be able to retrieve sensitive information related to the host, such as open UDP and TCP services lists, and detection of firewalls.
2	Medium	Intruders may be able to determine the operating system running on the host, and view banner versions.
3	Serious	Intruders may be able to detect highly sensitive data, such as global system user lists.