Aperia Compliance
An IXOPAY Company

Aperia - ASV Scan Report Vulnerability Details

LEAWOOD PRES

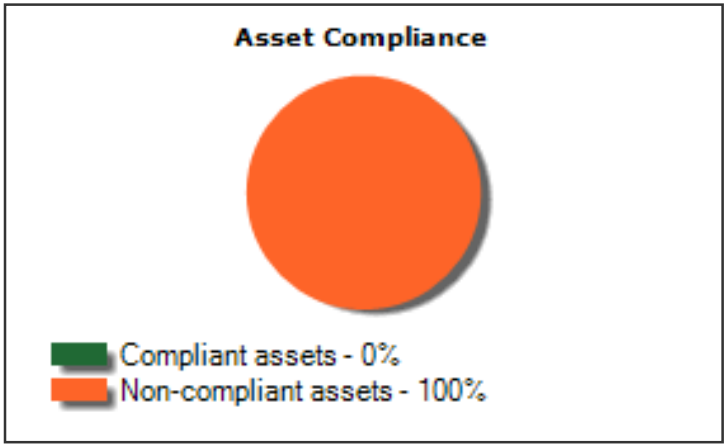
Audited on June 15, 2026. Reported on June 15, 2026

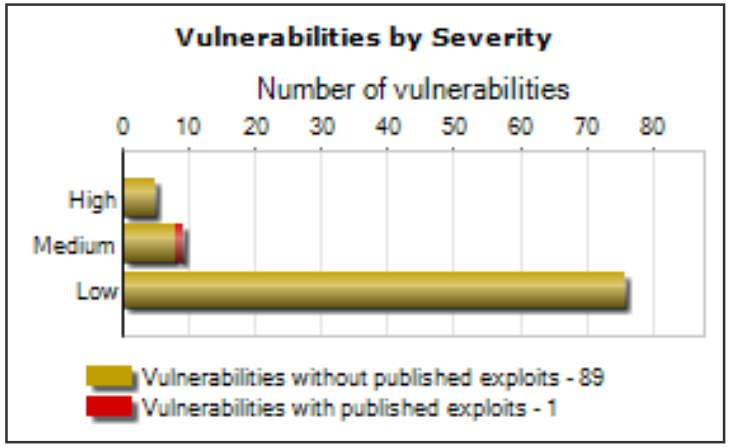
Table of Contents

Part 1. Scan Information

Scan Customer Company: LEAWOOD PRES	ASV Company: Aperia
Date scan was completed: June 15, 2026	Scan expiration date: September 13, 2026

Asset and Vulnerabilities Compliance Overview





Part 2. Vulnerability Details

Part 2a. High These vulnerabilities must be corrected and the environment must be re-scanned after the corrections. Organizations should take a risk-based approach to correct these types of vulnerabilities, starting with the ones having the highest CVSS scores.

Part 2a-1. 15164 - ISC BIND Depletion of CPU Resources Vulnerability (CVE-2024-1975) (CVE-2024-1975)

Severity	High
CVSS Score	7.5
Description	ISC BIND (Berkley Internet Domain Name) is an implementation of DNS protocols. Affected versions: BIND 9.0.0 -> 9.11.37 BIND 9.16.0 -> 9.16.50 BIND 9.18.0 -> 9.18.27 BIND 9.19.0 -> 9.19.24 BIND Supported Preview Edition 9.9.3-S1 -> 9.11.37-S1 BIND Supported Preview Edition 9.16.8-S1 -> 9.16.49-S1 BIND Supported Preview Edition 9.18.11-S1 -> 9.18.27-S1 Patched Versions: BIND 9.18.28 BIND 9.20.0 BIND Supported Preview Edition 9.18.28-S1 QID Detection Logic: This unauthenticated check detects vulnerable systems by fetching the version information from the BIND service using banner.

Affects

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
72.52.135.95	53/tcp	Linux 2.6	PASS	Vulnerable ISC BIND - 9.11.36-RedHat-9.11.36-16.el8_10.8 detected on port 53 over TCP.	ASV has modified the CVSS score
72.52.135.95	53/udp	Linux 2.6	PASS	Vulnerable ISC BIND - 9.11.36-RedHat-9.11.36-16.el8_10.8 detected on port 53 over UDP.	ASV has modified the CVSS score

Solution

Linux 2.6
Customers are advised to upgrade to the patched version latest release of CVE-2024-1975

Patch:
Following are links for downloading patches to fix the vulnerabilities:

CVE-2024-1975

Part 2a-2. 15163 - ISC BIND Slow Processing of Database Queries Vulnerability (CVE-2024-1737) (CVE-2024-1737)

Severity	High
CVSS Score	7.5
Description	ISC BIND (Berkley Internet Domain Name) is an implementation of DNS protocols. Affected versions: BIND 9.11.0 -> 9.11.37 BIND 9.16.0 -> 9.16.50 BIND 9.18.0 -> 9.18.27 BIND 9.19.0 -> 9.19.24 BIND Supported Preview Edition 9.11.4-S1 -> 9.11.37-S1

	BIND Supported Preview Edition 9.16.8-S1 -> 9.16.50-S1 BIND Supported Preview Edition 9.18.11-S1 -> 9.18.27-S1 Patched Versions: BIND 9.18.28 BIND 9.20.0 BIND Supported Preview Edition 9.18.28-S1 QID Detection Logic: This unauthenticated check detects vulnerable systems by fetching the version information from the BIND service using banner.

Affects

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
72.52.135.95	53/tcp	Linux 2.6	PASS	Vulnerable ISC BIND - 9.11.36-RedHat-9.11.36-16.el8_10.8 detected on port 53 over TCP.	ASV has modified the CVSS score
72.52.135.95	53/udp	Linux 2.6	PASS	Vulnerable ISC BIND - 9.11.36-RedHat-9.11.36-16.el8_10.8 detected on port 53 over UDP.	ASV has modified the CVSS score

Solution

Linux 2.6
Customers are advised to upgrade to the patched version latest release of CVE-2024-1737

Patch:
Following are links for downloading patches to fix the vulnerabilities:

CVE-2024-1737

Part 2a-3. 48169 - Remote Management Service Accepting Unencrypted Credentials Detected (FTP)

Severity	High
CVSS Score	7.3
Description	A remote management service that accepts unencrypted credentials was detected on the target host. Services like FTP with basic auth are checked.

Affects

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
72.52.135.95		Linux 2.6	FAIL	Service name: FTP on TCP port 21.	The vulnerability is not included in the NVD

Solution

Linux 2.6
If possible, use alternate services that provide encryption.
Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission.

Part 2b. Medium These vulnerabilities must be corrected and the environment must be re-scanned after the corrections. Organizations should take a risk-based approach to correct these types of vulnerabilities, starting with the ones having the highest CVSS scores.

Part 2b-1. 38628 - Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.0)

Severity	Medium
CVSS Score	6.5
Description	TLS is capable of using a multitude of ciphers (algorithms) to create the public and private key pairs. For example if TLSv1.0 uses either the RC4 stream cipher, or a block cipher in CBC mode. RC4 is known to have biases and the block cipher in CBC mode is vulnerable to the POODLE attack. TLSv1.0, if configured to use the same cipher suites as SSLv3, includes a means by which a TLS implementation can downgrade the connection to SSL v3.0, thus weakening security. A POODLE-type attack could also be launched directly at TLS without negotiating a downgrade. **This QID is an automatic PCI FAIL in accordance with the PCI standards.** **Further details can be found under:** **PCI: ASV Program Guide v3.1 (page 27)** **PCI: Use of SSL Early TLS and ASV Scans** NOTE: On March 31, 2021 Transport Layer Security (TLS) versions 1.0 (RFC 2246) and 1.1 (RFC 4346) are formally deprecated. Refer to Deprecating TLS 1.0 and TLS 1.1 QID Detection Logic (Unauthenticated): This QID is detected when the server successfully negotiates a TLS 1.0 handshake. Presence of TLS 1.0 alone is sufficient to flag this QID, independent of cipher strength. TLS 1.0 is deprecated (RFC 8996)

Affects

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
72.52.135.95	443/tcp	Linux 2.6	FAIL	TLSv1.0 is supported	The vulnerability is not included in the NVD

Solution

Linux 2.6
Disable the use of TLSv1.0 protocol in favor of a cryptographically stronger protocol such as TLSv1.2. The following openssl commands can be used to do a manual test: openssl s_client -connect ip:port -tls1 If the test is successful, then the target support TLSv1

Part 2b-2. 86476 - Web Server Stopped Responding

Severity	Medium
CVSS Score	6.4
Description	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

Affects

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
72.52.135.95	443/tcp	Linux 2.6	PASS	The web server did not respond for 4 consecutive HTTP requests. After these, the service was still unable to connect to the web server 2 minutes later.	Acceptable Risk noted BY Chip Lewis: Risk rating has been reduced following ASV review of this vulnerability. ASV score 2.6. best-practice recommendation has been communicated - scan customer must confirm no active scan interference.
72.52.135.95	52227/tcp	Linux 2.6	PASS	The web server did not respond for 4 consecutive HTTP requests. After these, the service was still unable to connect to the web server 2 minutes later.	Acceptable Risk noted BY Chip Lewis: Risk rating has been reduced following ASV review of this vulnerability. ASV score 2.6. best-

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
					practice recommendation has been communicated - scan customer must confirm no active scan interference.
72.52.135.95	52228/tcp	Linux 2.6	PASS	The web server did not respond for 4 consecutive HTTP requests. After these, the service was still unable to connect to the web server 2 minutes later.	Acceptable Risk noted BY Chip Lewis: Risk rating has been reduced following ASV review of this vulnerability. ASV score 2.6. best-practice recommendation has been communicated - scan customer must confirm no active scan interference.
72.52.135.95	52229/tcp	Linux 2.6	PASS	The web server did not respond for 4 consecutive HTTP requests. After these, the service was still unable to connect to the web server 2 minutes later.	Acceptable Risk noted BY Chip Lewis: Risk rating has been reduced following ASV review of this vulnerability. ASV score 2.6. best-practice recommendation has been communicated - scan customer must confirm no active scan interference.
72.52.135.95	80/tcp	Linux 2.6	PASS	The web server did not respond for 4 consecutive HTTP requests. After these, the service was still unable to connect to the web server 2 minutes later.	Acceptable Risk noted BY Chip Lewis: Risk rating has been reduced following ASV review of this vulnerability. ASV score 2.6. best-practice recommendation has been communicated - scan customer must confirm no active scan interference.
72.52.135.95	8443/tcp	Linux 2.6	PASS	The web server did not respond for 4 consecutive HTTP requests. After these, the service was still unable to connect to the web server 2 minutes later.	Acceptable Risk noted BY Chip Lewis: Risk rating has been reduced following ASV review of this vulnerability. ASV score 2.6. best-practice recommendation has been communicated - scan customer must confirm no active scan interference.

Solution

Linux 2.6
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.

Part 2b-3. 38229 - Service Stopped Responding

Severity	Medium
CVSS Score	5.0
Description	The service/daemon listening on the port shown stopped responding to TCP connection attempts during the scan. For more details about this QID, please review the following Qualys KB article:

Affects

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
72.52.135.95	2079/tcp	Linux 2.6	FAIL	3 consecutive connection attempts failed after a total number of 2 successful connections.	The vulnerability is not included in the NVD

Solution

Linux 2.6
This QID can be posted for a number of reasons (e.g., service crash, bandwidth utilization, or a device with IPS-like behavior).

If the service has crashed, report the incident to Customer Support or your QualysGuard re-seller, and stop scanning the service's listening port until the issue is resolved.

If the issue is bandwidth related, modify the Qualys performance settings to lower the scan impact.

If you do not find any service/daemon listening on this port, it may be a dynamic port and you may ignore this report.

This is posted as a PCI fail since the service stopped responding. Further checks were not launched for that service and therefore the PCI assessment was incomplete.

Part 2b-4. 82003 - ICMP Timestamp Request (CVE-1999-0524)

Severity	Medium
CVSS Score	4.0
Description	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.

Affects

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
72.52.135.95		Linux 2.6	PASS	Timestamp of host (network byte ordering):	

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
				16:18:46 GMT	

Solution

Linux 2.6
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.

Part 2c. Low Organizations are encouraged, but not required, to correct these vulnerabilities.

Part 2c-1. 38794 - Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server Supports Transport Layer Security (TLSv1.1)

Severity	Low
CVSS Score	3.7
Description	The scan target supports version 1.1 of the TLS protocol. That version is in the process of being deprecated and is no longer recommended. Instead the newer versions 1.2 and/or 1.3 should be used. The TLSv1.1 protocol itself does not have any currently exploitable vulnerabilities. However some vendor implementations of TLSv1.1 have weaknesses which may be exploitable. This QID is posted as potential, when servers require client certificates and we cannot complete the handshake.

	NOTE: On March 31, 2021 Transport Layer Security (TLS) versions 1.0 (RFC 2246) and 1.1 (RFC 4346) are formally deprecated. Refer to Deprecating TLS 1.0 and TLS 1.1 QID Detection Logic (Unauthenticated): This QID is detected when the server accepts a TLS 1.1 handshake. Even though TLS 1.1 has no known direct vulnerabilities, it is deprecated and reported when supported or inferred during the handshake. TLS 1.1 is formally deprecated (RFC 8996)

Affects

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
72.52.135.95	443/tcp	Linux 2.6	PASS	TLSv1.1 is supported	The vulnerability is not included in the NVD

Solution

Linux 2.6
Disable the use of TLSv1.1 protocol in favor of a cryptographically stronger protocol such as TLSv1.2. The following openssl commands can be used to do a manual test: openssl s_client -connect ip:port -tls1_1 If the test is successful, then the target support TLSv1.1

Part 2c-2. 45426 - Scan Activity per Port

Severity	Low
CVSS Score	0.0
Description	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.

Affects

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
72.52.135.95		Linux 2.6	PASS	Protocol Port Time TCP 21 0:12:53 TCP 25 0:15:10 TCP 53 0:01:30 TCP 80 1:36:48 TCP 110 0:01:48 TCP 143 0:01:24 TCP 443 3:11:53 TCP 2079 0:03:22 TCP 8443 2:59:32 TCP 52227 0:22:40 TCP 52228 0:19:43 TCP 52229 0:22:49 UDP 53 0:00:17	The vulnerability is not included in the NVD

Solution

Linux 2.6
N/A

Part 2c-3. 45038 - Host Scan Time - Scanner

Severity	Low
CVSS Score	0.0
Description	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.

Affects

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
72.52.135.95		Linux 2.6	PASS	Scan duration: 11031 seconds Start time: Mon, Jun 15 2026, 16:16:49 GMT End time: Mon, Jun 15 2026, 19:20:40 GMT	The vulnerability is not included in the NVD

Solution

Linux 2.6
N/A

Part 2c-4. 45006 - Traceroute

Severity	Low
CVSS Score	0.0
Description	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.

Affects

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
72.52.135.95		Linux 2.6	PASS	Hops IP Round Trip Time Probe Port 1 139.87.10.33 1.32ms ICMP	The vulnerability is not included in the NVD

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
				2 4.15.10.202 1.72ms ICMP 3 4.15.10.201 2.24ms ICMP 4 *.*.*.* 0.00ms Other 80 5 4.14.100.86 57.76ms ICMP 6 209.59.157.144 57.51ms ICMP 7 209.59.157.111 76.50ms ICMP 8 69.167.128.153 63.73ms ICMP 9 72.52.135.95 61.69ms TCP 80	

Solution

Linux 2.6
N/A

Part 2c-5. 45005 - Internet Service Provider

Severity	Low
CVSS Score	0.0
Description	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.

Affects

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
72.52.135.95		Linux 2.6	PASS	The ISP network handle is: LIQUIDWEB ISP Network description: Liquid Web, L.L.C	The vulnerability is not included in the NVD

Solution

Linux 2.6
N/A

Part 2c-6. 6 - DNS Host Name

Severity	Low
CVSS Score	0.0
Description	The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

Affects

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
72.52.135.95		Linux 2.6	PASS	IP address Host name 72.52.135.95 leawoodpres.org 72.52.135.95 host3.ministrydesigns.org	The vulnerability is not included in the NVD

Solution

Linux 2.6
N/A

Part 2c-7. 42017 - Remote Access or Management Service Detected

Severity	Low
CVSS Score	0.0
Description	A remote access or remote management service was detected. If such a service is accessible to malicious users it can be used to carry different type of attacks. Malicious users could try to brute force credentials or collect additional information on the service which could enable them in crafting further attacks. The Results section includes information on the remote access service that was found on the target. Services like Telnet, Rlogin, SSH, windows remote desktop, pcAnywhere, Citrix Management Console, Remote Admin (RAdmin), VNC, OPENVPN and ISAKMP are checked.

Affects

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
72.52.135.95		Linux 2.6	PASS	Service name: FTP on TCP port 21.	The vulnerability is not included in the NVD

Solution

Linux 2.6
Expose the remote access or remote management services only to the system administrators or intended users of the system.

Part 2c-8. 82004 - Open UDP Services List

Severity	Low

CVSS Score	0.0
Description	A port scanner was used to draw a map of all the UDP services on this host that can be accessed from the Internet. Note that if the host is behind a firewall, there is a small chance that the list includes a few ports that are filtered or blocked by the firewall but are not actually open on the target host. This (false positive on UDP open ports) may happen when the firewall is configured to reject UDP packets for most (but not all) ports with an ICMP Port Unreachable packet. This may also happen when the firewall is configured to allow UDP packets for most (but not all) ports through and filter/block/drop UDP packets for only a few ports. Both cases are uncommon.

Affects

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
72.52.135.95		Linux 2.6	PASS	Port IANA Assigned Ports/Services Description Service Detected 53 domain Domain Name Server named udp	The vulnerability is not included in the NVD

Solution

Linux 2.6
Shut down any unknown or unused service on the list. If you have difficulty working 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.

Part 2c-9. 45039 - Host Names Found

Severity	Low
CVSS Score	0.0
Description	The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

Affects

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
72.52.135.95		Linux 2.6	PASS	Host Name Source leawoodpres.org User-provided DNS host3.ministrydesigns.org FQDN	The vulnerability is not included in the NVD

Solution

Linux 2.6
N/A

Part 2c-10. 82023 - Open TCP Services List

Severity	Low
CVSS Score	0.0
Description	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).

Affects

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
72.52.135.95		Linux 2.6	PASS	Port IANA Assigned Ports/Services Descripti on Service Detected OS On Redirected Port	The vulnerability is not included in the NVD

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
				21 ftp File Transfer [Control] ftp 25 smtp Simple Mail Transfer smtp 53 domain Domain Name Server DNS Server 80 www-http World Wide Web HTTP http 110 pop3 Post Office Protocol - Version 3 pop3 143 imap Internet Message Access Protocol imap 443 https http protocol over TLS/SSL http over ssl 2079 unknown unknown unknown 8443 unknown unknown http over ssl 52227 unknown unknown http over ssl 52228 unknown unknown http 52229 unknown unknown http over ssl	

Solution

Linux 2.6
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.

Part 2c-11. 82040 - ICMP Replies Received

Severity	Low
CVSS Score	0.0
Description	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.

Affects

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
72.52.135.95		Linux 2.6	PASS	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 16:18:46 GMT Unreachable (type=3 code=3) UDP Port 443 Port Unreachable Unreachable (type=3 code=3) UDP Port 80 Port Unreachable	The vulnerability is not included in the NVD

Solution

Linux 2.6
N/A

Part 2c-12. 34011 - Firewall Detected

Severity	Low
CVSS Score	0.0
Description	A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

Affects

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
72.52.135.95		Linux 2.6	PASS	Some of the ports filtered by the firewall are: 22, 23, 111, 135, 445, 1, 7, 11, 67, 79. Listed below are the ports filtered by the fire wall. No response has been received when any of these ports are probed. 1-19,22-24,26-52,54-79,81-109,111-142,144-442,444-2078,2080-6128,6130-8442,8444-52226,52230-65535	The vulnerability is not included in the NVD

Solution

Linux 2.6
N/A

Part 2c-13. 150018 - Connection Error Occurred During Application Scan

Severity	Low
CVSS Score	0.0

Description	The following are some of the possible reasons for the timeouts or connection errors: 1. A disturbance in network connectivity between the scanner and the application occurred. 2. The web server or application server hosting the application was taken down in the midst of a scan. 3. The web application experienced an overload, possibly due to load generated by the scan. 4. An error occurred in the SSL/TLS handshake (applies to HTTPS web applications only). 5. A security device, such as an IDS/IPS or web application firewall (WAF), began to drop or reject the HTTP connections from the scanner. 6. Very large files like PDFs, videos, etc. are present on the site and caused timeouts when accessed by the scanner.

Affects

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
72.52.135.95	443/tcp	Linux 2.6	PASS	Total number of unique links that encountered timeout errors: 8 Links with highest number of timeouts: 1 https://72.52.135.95/ 1 https://72.52.135.95/../ 1 https://72.52.135.95/IUa6u6kgZuMQ.html 1 https://72.52.135.95/. 1 https://72.52.135.95/icons/small/ 1 https://72.52.135.95/src/ 1 https://72.52.135.95/v1/models 1 https://72.52.135.95/crossdomain.xml Phase wise summary of timeout and connection errors encountered: ePhaseCrawl : 7 0 ePhaseTest : 1 0	The vulnerability is not included in the NVD
72.52.135.95	52227/tcp	Linux 2.6	PASS	Total number of unique links that encountered connection errors: 8 Links with highest number of connection err	The vulnerability is not included in the NVD

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
				ors: 1 https://72.52.135.95:52227/icons/small/ 1 https://72.52.135.95:52227/v1/models 1 https://72.52.135.95:52227/ 1 https://72.52.135.95:52227/. 1 https://72.52.135.95:52227/../ 1 https://72.52.135.95:52227/src/ 1 https://72.52.135.95:52227/crossdomain.xml 1 https://72.52.135.95:52227/6u6kgZuMQWo5.html Phase wise summary of timeout and connection errors encountered: ePhaseCrawl : 0 7 ePhaseTest : 0 1	
72.52.135.95	52228/tcp	Linux 2.6	PASS	Total number of unique links that encountered connection errors: 8 Links with highest number of connection errors: 1 http://72.52.135.95:52228/../ 1 http://72.52.135.95:52228/icons/small/ 1 http://72.52.135.95:52228/. 1 http://72.52.135.95:52228/src/ 1 http://72.52.135.95:52228/v1/models 1 http://72.52.135.95:52228/ 1 http://72.52.135.95:52228/IUa6u6kgZuMQ.html 1 http://72.52.135.95:52228/crossdomain.xml Phase wise summary of timeout and connection errors encountered:	The vulnerability is not included in the NVD

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
				ePhaseCrawl : 0 7 ePhaseTest : 0 1	
72.52.135.95	52229/tcp	Linux 2.6	PASS	Total number of unique links that encountered connection errors: 8 Links with highest number of connection errors: 1 https://72.52.135.95:52229/. 1 https://72.52.135.95:52229/v1/models 1 https://72.52.135.95:52229/../ 1 https://72.52.135.95:52229/src/ 1 https://72.52.135.95:52229/ 1 https://72.52.135.95:52229/Ua6u6kgZuMQW.html 1 https://72.52.135.95:52229/icons/small/ 1 https://72.52.135.95:52229/crossdomain.xml Phase wise summary of timeout and connection errors encountered: ePhaseCrawl : 0 7 ePhaseTest : 0 1	The vulnerability is not included in the NVD
72.52.135.95	8443/tcp	Linux 2.6	PASS	Total number of unique links that encountered timeout errors: 8 Links with highest number of timeouts: 1 https://72.52.135.95:8443/../ 1 https://72.52.135.95:8443/ 1 https://72.52.135.95:8443/v1/models 1 https://72.52.135.95:8443/Ua6u6kgZuMQW.html 1 https://72.52.135.95:8443/icons/small/ 1 https://72.52.135.95:8443/src/ 1 https://72.52.135.95:8443/crossdomain.xml	The vulnerability is not included in the NVD

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
				1 https://72.52.135.95:8443/. Phase wise summary of timeout and connec tion errors encountered: ePhaseCrawl : 7 0 ePhaseTest : 1 0	

Solution

Linux 2.6
First, confirm that the server was not taken down in the midst of the scan. After that, investigate the root cause by reviewing the listed links and examining web server logs, application server logs, or IDS/IPS/WAF logs. If the errors are caused due to load generated by the scanner then try reducing the scan intensity (this could increase the scan duration). If the errors are due to specific URLs being tested by the scanner or due to specific form data sent by the scanner, then configure exclude lists in the scan configuration as needed to avoid such requests. If timeouts or connection errors are a persistent issue but you want the scan to run to completion, change the Behavior Settings in the option profile to increase the error thresholds or disable the error checks entirely.

Part 2c-14. 150021 - Scan Diagnostics

Severity	Low
CVSS Score	0.0
Description	This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

Affects

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
72.52.135.95	443/tcp	Linux 2.6	PASS	Ineffective Session Protection. no tests enabled. HSTS Analysis no tests enabled. Collected 1 links overall in 0 hours 7 minutes duration. No links were discovered during the crawl phase. Duration of Crawl Time: 420.00 (seconds) Duration of Test Phase: 60.00 (seconds) Total Scan Time: 480.00 (seconds) Total requests made: 8 Average server response time: 0.00 seconds Average browser load time: 0.00 seconds HTML form authentication unavailable, no WEBAPP entry found	The vulnerability is not included in the NVD
72.52.135.95	52227/tcp	Linux 2.6	PASS	Ineffective Session Protection. no tests enabled. HSTS Analysis no tests enabled. Collected 1 links overall in 0 hours 1 minutes duration. No links were discovered during the crawl phase. Duration of Crawl Time: 71.00 (seconds) Duration of Test Phase: 10.00 (seconds) Total Scan Time: 81.00 (seconds) Total requests made: 8 Average server response time: 0.00 seconds Average browser load time: 0.00 seconds HTML form authentication unavailable, no WEBAPP entry found	The vulnerability is not included in the NVD

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
72.52.135.95	52228/tcp	Linux 2.6	PASS	Ineffective Session Protection. no tests enabled. HSTS Analysis no tests enabled. Collected 1 links overall in 0 hours 1 minutes duration. No links were discovered during the crawl phase. Duration of Crawl Time: 71.00 (seconds) Duration of Test Phase: 10.00 (seconds) Total Scan Time: 81.00 (seconds) Total requests made: 8 Average server response time: 0.00 seconds Average browser load time: 0.00 seconds HTML form authentication unavailable, no WEBAPP entry found	The vulnerability is not included in the NVD
72.52.135.95	52229/tcp	Linux 2.6	PASS	Ineffective Session Protection. no tests enabled. HSTS Analysis no tests enabled. Collected 1 links overall in 0 hours 1 minutes duration. No links were discovered during the crawl phase. Duration of Crawl Time: 71.00 (seconds) Duration of Test Phase: 10.00 (seconds) Total Scan Time: 81.00 (seconds) Total requests made: 8 Average server response time: 0.00 seconds Average browser load time: 0.00 seconds HTML form authentication unavailable, no WEBAPP entry found	The vulnerability is not included in the NVD

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
72.52.135.95	80/tcp	Linux 2.6	PASS	Target web application page http://72.52.135.95/ fetched. Status code:200, Content-Type:text/html, load time:177 milliseconds. Ineffective Session Protection. no tests enabled. Batch #0 CMSDetection: estimated time < 1 minute (1 tests, 1 inputs) [CMSDetection phase] : No potential CMS found using Blind Elephant algorithm. Aborting the CMS Detection phase CMSDetection: 1 vulnsigs tests, completed 38 requests, 3 seconds. Completed 38 requests of 38 estimated requests (100%). All tests completed. HSTS Analysis no tests enabled. Collected 3 links overall in 0 hours 1 minutes duration. Batch #0 BannersVersionReporting: estimated time < 1 minute (1 tests, 1 inputs) BannersVersionReporting: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 1 estimated requests (0%). All tests completed. Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 2) + files:(0 x 2) + directories:(9 x 3) + paths:(0 x 5) = total (27) Batch #0 WS Directory Path manipulation: estimated time < 1 minute (9 tests, 5 inputs) WS Directory Path manipulation: 9 vulnsigs tests, completed 27 requests, 1 seconds. Completed 27 requests of 27 estimated request	The vulnerability is not included in the NVD

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
				s (100%). All tests completed. WSEnumeration no tests enabled. Batch #1 No links or forms to test Batch #2 WebCgiOob: estimated time < 1 minute (172 tests, 1 inputs) Batch #2 WebCgiOob: 172 vulnsigs tests, completed 114 requests, 3 seconds. Completed 114 requests of 485 estimated requests (23.5052%). All tests completed. XXE tests no tests enabled. HTTP call manipulation no tests enabled. SSL Downgrade. no tests enabled. Open Redirect no tests enabled. CSRF no tests enabled. Batch #2 File Inclusion analysis: estimated time < 1 minute (1 tests, 3 inputs) Batch #2 File Inclusion analysis: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 3 estimated requests (0%). All tests completed. Batch #2 Cookie manipulation: estimated time < 1 minute (47 tests, 0 inputs) Batch #2 Cookie manipulation: 47 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute. Batch #2 Header manipulation: estimated time < 1 minute (47 tests, 2 inputs) Batch #2 Header manipulation: 47 vulnsigs tests, completed 242 requests, 11 seconds. Completed 242 requests of 260 estimated requests (93.0769%). XSS optimization removed 116 links. All tests completed.	

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
				Batch #2 shell shock detector: estimated tim e < 1 minute (1 tests, 2 inputs) Batch #2 shell shock detector: 1 vulnsigs tes ts, completed 2 requests, 1 seconds. Compl eted 2 requests of 2 estimated requests (10 0%). All tests completed. Batch #2 shell shock detector(form): estimat ed time < 1 minute (1 tests, 0 inputs) Batch #2 shell shock detector(form): 1 vulnsi gs tests, completed 0 requests, 0 seconds. No tests to execute. httpoxy no tests enabled. Static Session ID no tests enabled. Login Brute Force no tests enabled. Login Brute Force manipulation estimated ti me: no tests enabled Insecurely Served Credential Forms no tests enabled. Cookies Without Consent no tests enabled. Batch #3 HTTP Time Bandit: estimated time < 1 minute (1 tests, 10 inputs) Batch #3 HTTP Time Bandit: 1 vulnsigs test s, completed 0 requests, 0 seconds. No test s to execute. Path manipulation: Estimated requests (payl oads x links): files with extension:(0 x 2) + fil es:(0 x 2) + directories:(5 x 3) + paths:(10 x 5) = total (65) Batch #3 Path XSS manipulation: estimated time < 1 minute (15 tests, 5 inputs) Batch #3 Path XSS manipulation: 15 vulnsig s tests, completed 64 requests, 0 seconds.	

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
				Completed 64 requests of 65 estimated requ ests (98.4615%). All tests completed. Tomcat Vuln manipulation no tests enabled. Time based path manipulation no tests enab led. Path manipulation: Estimated requests (payl oads x links): files with extension:(0 x 2) + fil es:(4 x 2) + directories:(103 x 3) + paths:(5 x 5) = total (342) Batch #3 Path manipulation: estimated time < 1 minute (112 tests, 5 inputs) Batch #3 Path manipulation: 112 vulnsigs te sts, completed 335 requests, 4 seconds. Co mpleted 335 requests of 342 estimated requ ests (97.9532%). All tests completed. WebCgiHrsTests: no test enabled Batch #3 WebCgiGeneric: estimated time &l t; 10 minutes (2264 tests, 1 inputs) Batch #3 WebCgiGeneric: 2264 vulnsigs tes ts, completed 3555 requests, 96 seconds. C ompleted 3555 requests of 16920 estimated requests (21.0106%). All tests completed. Batch #3 WebCgiTimebased: estimated time < 1 minute (2 tests, 1 inputs) Batch #3 WebCgiTimebased: 2 vulnsigs test s, completed 3 requests, 1 seconds. Comple ted 3 requests of 15 estimated requests (2 0%). All tests completed. Batch #3 Web Cache Poisoning: estimated ti me < 1 minute (6 tests, 6 inputs) Batch #3 Web Cache Poisoning: 6 vulnsigs t ests, completed 16 requests, 1 seconds. Co	

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
				mpleted 16 requests of 36 estimated requests (44.4444%). All tests completed. Batch #4 No tests to perform Batch #5 No tests to perform Duration of Crawl Time: 77.00 (se	
72.52.135.95	8443/tcp	Linux 2.6	PASS	Ineffective Session Protection. no tests enabled. HSTS Analysis no tests enabled. Collected 1 links overall in 0 hours 7 minutes duration. No links were discovered during the crawl phase. Duration of Crawl Time: 421.00 (seconds) Duration of Test Phase: 60.00 (seconds) Total Scan Time: 481.00 (seconds) Total requests made: 8 Average server response time: 0.00 seconds Average browser load time: 0.00 seconds HTML form authentication unavailable, no WEBAPP entry found	The vulnerability is not included in the NVD

Solution

Linux 2.6
No action is required.

Part 2c-15. 150020 - Links Rejected By Crawl Scope or Exclusion List

Severity	Low

CVSS Score	0.0
Description	One or more links were not crawled because of an explicit rule to exclude them. This also occurs if a link is malformed. Exclude list and Include list entries can cause links to be rejected. If a scan is limited to a specific starting directory, then links outside that directory will neither be crawled or tested. Links that contain a host name or IP address different from the target application are considered external links and not crawled by default; those types of links are not listed here. This often happens when the scope of a scan is limited to the directory of the starting URL. The scope can be changed in the Web Application Record. During the test phase, some path-based tests may be rejected if the scan is limited to the directory of the starting URL and the test would fall outside that directory. In these cases, the number of rejected links may be too high to list in the Results section.

Affects

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
72.52.135.95	443/tcp	Linux 2.6	PASS	Links not permitted: (This list includes links from QIDs: 150010,150041,150143,150170) IP based excluded links:	The vulnerability is not included in the NVD
72.52.135.95	52227/tcp	Linux 2.6	PASS	Links not permitted: (This list includes links from QIDs: 150010,150041,150143,150170) IP based excluded links:	The vulnerability is not included in the NVD
72.52.135.95	52228/tcp	Linux 2.6	PASS	Links not permitted: (This list includes links from QIDs: 150010,150041,150143,150170) IP based excluded links:	The vulnerability is not included in the NVD
72.52.135.95	52229/tcp	Linux 2.6	PASS	Links not permitted: (This list includes links from QIDs: 150010,150041,150143,150170) IP based excluded links:	The vulnerability is not included in the NVD

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
72.52.135.95	80/tcp	Linux 2.6	PASS	Links not permitted: (This list includes links from QIDs: 150010,150041,150143,150170) External links discovered: https://go.cpanel.net/cleardnscache https://go.cpanel.net/privacy https://cpanel.net/?utm_source=cpanelwhm&utm_medium=cplogo&utm_content=logolink&utm_campaign=cpanelwhmreferral http://cpanel.com/?utm_source=cpanelwhm&utm_medium=cplogo&utm_content=logolink&utm_campaign=500referral IP based excluded links:	The vulnerability is not included in the NVD
72.52.135.95	8443/tcp	Linux 2.6	PASS	Links not permitted: (This list includes links from QIDs: 150010,150041,150143,150170) IP based excluded links:	The vulnerability is not included in the NVD

Solution

Linux 2.6
A link might have been intentionally matched by a exclude or include list entry. Verify that no links in this list were unintentionally rejected.

Part 2c-16. 150009 - Links Crawled

Severity	Low
CVSS Score	0.0

Description	The list of unique links crawled and HTML forms submitted by the scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined. NOTE: This list also includes: - All the unique links that are reported in QID 150140 (Redundant links/URL paths crawled and not crawled) - All the forms reported in QID 150152 (Forms Crawled) - All the forms in QID 150115 (Authentication Form Found) - Certain requests from QID 150172 (Requests Crawled)

Affects

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
72.52.135.95	443/tcp	Linux 2.6	PASS	Duration of crawl phase (seconds): 420.00 Number of links: 0 (This number excludes form requests and links re-requested during authentication.) No links were crawled during this scan. Review the scan configuration and target web application for errors. When possible, additional diagnostic information will be reported in QID 150021.	The vulnerability is not included in the NVD
72.52.135.95	52227/tcp	Linux 2.6	PASS	Duration of crawl phase (seconds): 71.00 Number of links: 0 (This number excludes form requests and links re-requested during authentication.) No links were crawled during this scan. Review the scan configuration and target web application for errors. When possible, additional diagnostic information will be reported in QID 150021.	The vulnerability is not included in the NVD
72.52.135.95	52228/tcp	Linux 2.6	PASS	Duration of crawl phase (seconds): 71.00 Number of links: 0	The vulnerability is not included in the NVD

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
				(This number excludes form requests and links re-requested during authentication.) No links were crawled during this scan. Review the scan configuration and target web application for errors. When possible, additional diagnostic information will be reported in QID 150021.	
72.52.135.95	52229/tcp	Linux 2.6	PASS	Duration of crawl phase (seconds): 71.00 Number of links: 0 (This number excludes form requests and links re-requested during authentication.) No links were crawled during this scan. Review the scan configuration and target web application for errors. When possible, additional diagnostic information will be reported in QID 150021.	The vulnerability is not included in the NVD
72.52.135.95	80/tcp	Linux 2.6	PASS	Duration of crawl phase (seconds): 77.00 Number of links: 3 (This number excludes form requests and links re-requested during authentication.) http://72.52.135.95/ http://72.52.135.95/cgi-sys/defaultwebpage.cgi http://72.52.135.95/img-sys/error-bg-left.png	The vulnerability is not included in the NVD
72.52.135.95	8443/tcp	Linux 2.6	PASS	Duration of crawl phase (seconds): 421.00 Number of links: 0 (This number excludes form requests and links re-requested during authentication.) No links were crawled during this scan. Review the scan configuration and target web application for errors. When possible, additiona	The vulnerability is not included in the NVD

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
				l diagnostic information will be reported in QI D 150021.	

Solution

Linux 2.6
N/A

Part 2c-17. 86672 - List of Web Directories

Severity	Low
CVSS Score	0.0
Description	Based largely on the HTTP reply code, the following directories are most likely present on the host.

Affects

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
72.52.135.95	443/tcp	Linux 2.6	PASS	Directory Source /webmail/ brute force /news/ brute force	The vulnerability is not included in the NVD
72.52.135.95	52228/tcp	Linux 2.6	PASS	Directory Source /cgi/ brute force /images/ brute force /img/ brute force /login/ brute force	The vulnerability is not included in the NVD

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
72.52.135.95	80/tcp	Linux 2.6	PASS	Directory Source /webmail/ brute force	The vulnerability is not included in the NVD

Solution

Linux 2.6
N/A

Part 2c-18. 86671 - List of Web Directories Requiring Authentication

Severity	Low
CVSS Score	0.0
Description	The service has identified a list of Web directories which require authentication to access.

Affects

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
72.52.135.95	52228/tcp	Linux 2.6	PASS	Directories Requiring Authentication /login/	The vulnerability is not included in the NVD

Solution

Linux 2.6
N/A

Part 2c-19. 38597 - Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance

Severity	Low
CVSS Score	0.0
Description	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.

Affects

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
72.52.135.95	21/tcp	Linux 2.6	PASS	my version target version 0304 rejected 0399 rejected 0400 rejected 0499 rejected	The vulnerability is not included in the NVD
72.52.135.95	25/tcp	Linux 2.6	PASS	my version target version 0304 rejected 0399 rejected 0400 rejected 0499 rejected	The vulnerability is not included in the NVD
72.52.135.95	443/tcp	Linux 2.6	PASS	my version target version 0304 rejected 0399 rejected 0400 rejected 0499 rejected	The vulnerability is not included in the NVD
72.52.135.95	52227/tcp	Linux 2.6	PASS	my version target version 0304 rejected 0399 rejected	The vulnerability is not included in the NVD

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
				0400 rejected 0499 rejected	
72.52.135.95	52229/tcp	Linux 2.6	PASS	my version target version 0304 rejected 0399 rejected 0400 rejected 0499 rejected	The vulnerability is not included in the NVD
72.52.135.95	8443/tcp	Linux 2.6	PASS	my version target version 0304 rejected 0399 rejected 0400 rejected 0499 rejected	The vulnerability is not included in the NVD

Solution

Linux 2.6
N/A

Part 2c-20. 86000 - Web Server Version

Severity	Low
CVSS Score	0.0
Description	A web server is server software, or hardware dedicated to running this software, that can satisfy client requests on the World Wide Web.

Affects

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
72.52.135.95	52228/tcp	Linux 2.6	PASS	Server Version Server Banner Microsoft-IIS/4.0 _	The vulnerability is not included in the NVD

Solution

Linux 2.6
N/A

Part 2c-21. 150845 - Business logic abuse potential due to presence of external domains detected

Severity	Low
CVSS Score	0.0
Description	External domains detected in the application. Using external domains in an application introduces risk by potentially exposing the application to external threats and dependencies, which can be exploited for malicious purposes such as data exfiltration, phishing, or compromise of application integrity. These vulnerabilities arise from inadequate validation, reliance on unsecured external services, and the application's failure to enforce strict security controls over external interactions.

Affects

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
72.52.135.95	80/tcp	Linux 2.6	PASS	External domains could be involved in poten tial business logic abuse. cpanel.com cpanel.net go.cpanel.net	The vulnerability is not included in the NVD

Solution

Linux 2.6
Audit external domains accessed by your application. If possible launch scans against those.

Part 2c-22. 150010 - External Links Discovered

Severity	Low
CVSS Score	0.0
Description	External links discovered during the scan are listed in the Results section. These links were out of scope for the scan and were not crawled.

Affects

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
72.52.135.95	80/tcp	Linux 2.6	PASS	Number of links: 4 https://go.cpanel.net/cleardnscache https://go.cpanel.net/privacy https://cpanel.net/?utm_source=cpanelwhm&utm_medium=cplogo&utm_content=logolink&utm_campaign=cpanelwhmreferral http://cpanel.com/?utm_source=cpanelwhm&utm_medium=cplogo&utm_content=logolink&utm_campaign=500referral	The vulnerability is not included in the NVD

Solution

Linux 2.6
N/A

Part 2c-23. 86001 - SSL Web Server Version

Severity	Low
CVSS Score	0.0
Description	A web server is server software, or hardware dedicated to running this software, that can satisfy client requests on the World Wide Web.

Affects

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
72.52.135.95	443/tcp	Linux 2.6	PASS	Server Version Server Banner Microsoft-IIS/4.0 _	The vulnerability is not included in the NVD
72.52.135.95	52227/tcp	Linux 2.6	PASS	Server Version Server Banner Microsoft-IIS/4.0 _	The vulnerability is not included in the NVD
72.52.135.95	52229/tcp	Linux 2.6	PASS	Server Version Server Banner Microsoft-IIS/4.0 _	The vulnerability is not included in the NVD

Solution

Linux 2.6
N/A

Part 2c-24. 27113 - FTP Server Banner

Severity	Low
CVSS Score	0.0

Description	The following message is shown to all users logging on to your FTP server, including anonymous logins if they are allowed on your server.

Affects

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
72.52.135.95	21/tcp	Linux 2.6	PASS	220---------- Welcome to Pure-FTPd [privsep] [TLS] ---------- 220-You are user number 1 of 50 allowed. 220-Local time is now 12:20. Server port: 21. 220-This is a private system - No anonymous login 220-IPv6 connections are also welcome on this server. 220 You will be disconnected after 15 minutes of inactivity.	The vulnerability is not included in the NVD

Solution

Linux 2.6
If possible, edit the configuration files or recompile the server to restrict the type of information disclosed.

Part 2c-25. 50000 - POP3 Banner

Severity	Low
CVSS Score	0.0
Description	Post Office Protocol version 3 (POP3) is a standard mail protocol used to receive emails from a remote server to a local email client. POP3 allows you to download email messages on your local computer and read them even when you are offline.

Affects

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
72.52.135.95	110/tcp	Linux 2.6	PASS	+OK Dovecot ready.	The vulnerability is not included in the NVD

Solution

Linux 2.6
NA

Part 2c-26. 50010 - IMAP Banner

Severity	Low
CVSS Score	0.0
Description	IMAP (Internet Message Access Protocol) is a standard email protocol that stores email messages on a mail server, but allows the end user to view and manipulate the messages as though they were stored locally on the end user's computing device(s). QID Detection Logic: The QID checks for IMAP in the banner of the response.

Affects

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
72.52.135.95	143/tcp	Linux 2.6	PASS	* OK [CAPABILITY IMAP4rev1 LOGIN-REF ERRALS ID ENABLE IDLE SASL-IR LITER	The vulnerability is not included in the NVD

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
				AL+ STARTTLS LOGINDISABLED] Dovecot ready.	

Solution

Linux 2.6
N/A

Part 2c-27. 74042 - SMTP Banner

Severity	Low
CVSS Score	0.0
Description	The Simple Mail Transfer Protocol is a communication protocol for electronic mail transmission. QID Detection Logic: The QID checks for 220 status code in the banner of the response.

Affects

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
72.52.135.95	25/tcp	Linux 2.6	PASS	220-host3.ministrydesigns.org ESMTP Exim 4.99.4 #2 Mon, 15 Jun 2026 12:21:15 -0400 220-We do not authorize the use of this syst em to transport unsolicited, 220 and/or bulk e-mail.	The vulnerability is not included in the NVD

Solution

Linux 2.6
NA

Part 2c-28. 15001 - Named Daemon Version Number Disclosure Vulnerability

Severity	Low
CVSS Score	0.0
Description	Named is the daemon used to provide the DNS translation service.

Affects

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
72.52.135.95	53/tcp	Linux 2.6	PASS	9.11.36-RedHat-9.11.36-16.el8_10.8	The vulnerability is not included in the NVD

Solution

Linux 2.6
Unless it is required on this host, disable this feature.

Part 2c-29. 45017 - Operating System Detected

Severity	Low
CVSS Score	0.0

Description	Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report. 1) **TCP/IP Fingerprint**: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below. Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that of the firewall instead of the host being scanned. 2) **NetBIOS**: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB). 3) **PHP Info**: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information. 4) **SNMP**: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system.sysDescr" for the operating system.

Affects

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
72.52.135.95		Linux 2.6	PASS	Operating System Technique ID Linux 2.6 TCP/IP Fingerprint U6397:21	The vulnerability is not included in the NVD

Solution

Linux 2.6
Not applicable.

Part 2c-30. 48340 - Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.2)

Severity	Low
CVSS Score	0.0
Description	N/A

Affects

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
72.52.135.95	21/tcp	Linux 2.6	PASS	TLSv1.2 is supported	The vulnerability is not included in the NVD
72.52.135.95	25/tcp	Linux 2.6	PASS	TLSv1.2 is supported	The vulnerability is not included in the NVD
72.52.135.95	443/tcp	Linux 2.6	PASS	TLSv1.2 is supported	The vulnerability is not included in the NVD
72.52.135.95	52227/tcp	Linux 2.6	PASS	TLSv1.2 is supported	The vulnerability is not included in the NVD
72.52.135.95	52229/tcp	Linux 2.6	PASS	TLSv1.2 is supported	The vulnerability is not included in the NVD
72.52.135.95	8443/tcp	Linux 2.6	PASS	TLSv1.2 is supported	The vulnerability is not included in the NVD

Solution

Linux 2.6
N/A

Part 2c-31. 150606 - Scan Diagnostics Information

Severity	Low
CVSS Score	0.0
Description	Scan meta data will be reported under this QID. Number of links, parameters tested, total number of requests per phase, time required to finish and phase status.

Affects

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
72.52.135.95	443/tcp	Linux 2.6	PASS	No scan diagnostic metadata collected.	The vulnerability is not included in the NVD
72.52.135.95	52227/tcp	Linux 2.6	PASS	No scan diagnostic metadata collected.	The vulnerability is not included in the NVD
72.52.135.95	52228/tcp	Linux 2.6	PASS	No scan diagnostic metadata collected.	The vulnerability is not included in the NVD
72.52.135.95	52229/tcp	Linux 2.6	PASS	No scan diagnostic metadata collected.	The vulnerability is not included in the NVD
72.52.135.95	80/tcp	Linux 2.6	PASS	========== ========== ========== = SCAN EXECUTION SUMMARY ==========	The vulnerability is not included in the NVD

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
				========== ========== = ---------- ---------- CRAWLING PHASE ---------- ---------- Duration: 1m 17s Links Crawled: 3 Links Collected: 3 Average Response Time: 99ms ---------- ---------- TEST PHASE: CMSDetection ---------- ---------- Parameters: 3 Expected Requests: 38 Actual Requests: 38 Time Taken: 3s Average Response Time: 88ms Status: Completed - No potential CMS found ---------- ---------- TEST PHASE: BannersVersionReporting ---------- ---------- Parameters: 1 Payloads: 1 Expected Requests: 1 Actual Requests: 0	

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
				Time Taken: 0s Average Response Time: 0ms Status: Completed ---------- ---------- TEST PHASE: WS Directory Path manipulat ion ---------- ---------- Parameters: 5 Payloads: 9 Expected Requests: 27 Actual Requests: 27 Time Taken: 1s Average Response Time: 96ms Status: Completed ---------- ---------- TEST PHASE: WebCgiOob ---------- ---------- Parameters: 1 Payloads: 172 Expected Requests: 485 Actual Requests: 114 Time Taken: 3s Average Response Time: 187ms Status: Completed ---------- ---------- TEST PHASE: File Inclusion analysis ----------	

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
				---------- Parameters: 3 Payloads: 1 Expected Requests: 3 Actual Requests: 0 Time Taken: 0s Average Response Time: 0ms Status: Completed ---------- ---------- TEST PHASE: Cookie manipulation ---------- ---------- Status: No tests to execute. ---------- ---------- TEST PHASE: Header manipulation ---------- ---------- Parameters: 2 Payloads: 47 Expected Requests: 260 Actual Requests: 242 Time Taken: 11s Average Response Time: 256ms Status: Completed ---------- ---------- TEST PHASE: shell shock detector ---------- ---------- Parameters: 2	

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
				Payloads: 1 Expected Requests: 2 Actual Requests: 2 Time Taken: 1s Average Response Time: 140ms Status: Completed ---------- ---------- TEST PHASE: shell shock detector(form) ---------- ---------- Status: No tests to execute. ---------- ---------- TEST PHASE: HTTP Time Bandit ---------- ---------- Status: No tests to execute. ---------- ---------- TEST PHASE: Path XSS manipulation ---------- ---------- Para	
72.52.135.95	8443/tcp	Linux 2.6	PASS	No scan diagnostic metadata collected.	The vulnerability is not included in the NVD

Solution

Linux 2.6
Review scan data and adjust scan settings accordingly.

Part 2c-32. 150605 - Post requests count per phase

Severity	Low
CVSS Score	0.0
Description	This QID is informational reports number of POST requests per test phase.

Affects

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
72.52.135.95	443/tcp	Linux 2.6	PASS	POST Request Count Report ========== Total POST Requests: 0	The vulnerability is not included in the NVD
72.52.135.95	52227/tcp	Linux 2.6	PASS	POST Request Count Report ========== Total POST Requests: 0	The vulnerability is not included in the NVD
72.52.135.95	52228/tcp	Linux 2.6	PASS	POST Request Count Report ========== Total POST Requests: 0	The vulnerability is not included in the NVD
72.52.135.95	52229/tcp	Linux 2.6	PASS	POST Request Count Report ========== Total POST Requests: 0	The vulnerability is not included in the NVD
72.52.135.95	80/tcp	Linux 2.6	PASS	POST Request Count Report ========== Total POST Requests: 0	The vulnerability is not included in the NVD
72.52.135.95	8443/tcp	Linux 2.6	PASS	POST Request Count Report ========== Total POST Requests: 0	The vulnerability is not included in the NVD

Solution

Linux 2.6
If number of POST requests are higher, fine tune your web application scanning using redundant URLs, form redundancy or blacklist features.

Part 2c-33. 531006 - Cross Frame Scripting Protection Missing

Severity	Low
CVSS Score	0.0
Description	Cross-Frame Scripting is a web attack technique that exploits specific browser vulnerabilities to eavesdrop on users through JavaScript. This type of attack requires social engineering and depends on the browser selected, and is perceived as a minor web application security threat. Cross-Frame Scripting XFS is determined based on headers, when either Content Security Policy or X Frame Options are missing then XFS could be manifest in web applications.

Affects

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
72.52.135.95	80/tcp	Linux 2.6	PASS	Potential Cross-Frame Scripting (XFS) Exposure Detected The following pages lack anti-framing headers (X-Frame-Options and CSP frame-ancestors), which could potentially expose them to Cross-Frame Scripting attacks in legacy browsers. (Only first 10 such pages are reported) GET http://72.52.135.95/cgi-sys/defaultwebpage.cgi Response code: 200 Response headers:	The vulnerability is not included in the NVD

IP Address	Port	Instance	Compliance Status	Evidence	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
				Server: nginx Date: Mon, 15 Jun 2026 16:22:11 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding X-Content-Type-Options: nosniff X-Content-Type-Options: nosniff Strict-Transport-Security: max-age=31536000; includeSubDomains X-XSS-Protection: 1; mode=block X-XSS-Protection: 1; mode=block Cache-Control: max-age=600 Expires: Mon, 15 Jun 2026 16:32:11 GMT X-Nginx-Upstream-Cache-Status: MISS X-Server-Powered-By: Engintron Content-Encoding: gzip	

Solution

Linux 2.6
Since Cross-Frame Scripting vulnerabilities appear in web browsers, web application developers can only prevent frame embedding. There are three primary methods of protection. Since all of them are also used to protect against clickjacking, you can read all about them in our article How to Defend Against Clickjacking Attacks Framebusting, The legitimate website owner only needs to modify the web page HTML code. The Content-Security-Policy, with frame-ancestors header set to self. The legitimate website owner must modify web server configuration and have this header automatically included with every page. The X-Frame-Options header, The legitimate website owner must modify web server configuration and have this header automatically included with every page. Lastly, keep the browser updated all times.