

Sample Report

Vulnerability Assessment Report

ACME Web Production

Mapped to CERT-In Cyber Security Directions (April 2022)

RISK LEVEL	CRITICAL
SCAN START	13 Mar 2026 06:48 UTC
SCAN END	13 Mar 2026 07:05 UTC
FINDINGS	62 total · 22 actionable
TARGETS	1 host
REPORT DATE	13 Mar 2026 07:05 UTC
COMPLIANCE	CERT-In Guidelines

Executive Summary

Ogma

Vulnerability findings by severity



Priority Action Items

Top 4 Critical/High findings requiring immediate attention

#	FINDING	HOST	SEVERITY	CVSS	QUICK FIX
1	Apache HTTP Server < 2.4.60 Multiple Vulnerabilities - Linux	203.0.113.45	CRITICAL	9.8	Update to version 2.4.60 or later.
2	OpenBSD OpenSSH < 4.4p1, 8.5p1 - 9.7p1 RCE Vulnerability (regreSSHion)	203.0.113.45	HIGH	8.1	Update to version 9.8 or later.
3	Apache HTTP Server < 2.4.59 Multiple Vulnerabilities - Linux	203.0.113.45	HIGH	7.5	Update to version 2.4.59 or later.
4	Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSH, D(HE)ater)	203.0.113.45	HIGH	7.5	- DHE key exchange should be disabled if no other mitigation mechanism can be used and either elliptic-curve variant o...

Scan Details

SCAN NAME	ACME-Web-Production
START TIME	13 Mar 2026 06:48 UTC
END TIME	13 Mar 2026 07:05 UTC
TOTAL FINDINGS	62 (22 actionable, 40 informational)
HOSTS SCANNED	1
OVERALL RISK	CRITICAL
REPORT DATE	13 Mar 2026 07:05 UTC
PREPARED BY	Ogma Consulting Pvt Ltd
COMPLIANCE	CERT-In Guidelines

Targets Scanned

203.0.113.45

Compliance Mapping — CERT-In Guidelines



Mapped to CERT-In Cyber Security Directions (April 2022)

CERT-IN GUIDELINES

The following table maps scan findings to CERT-In Guidelines requirement areas. A non-zero count indicates findings that are relevant to that compliance requirement.

REQ ID	REQUIREMENT AREA	DESCRIPTION	FINDINGS
6hr Reporting	Incident Reporting	Mandatory reporting of cyber incidents to CERT-In within 6 hours.	0
Network Security	Network Hardening	Secure network configuration, segmentation, and perimeter controls.	0
Access Control	Access Management	Strong authentication, VPN, and privileged access controls.	18
Patch Mgmt	Patch & Vulnerability Management	Timely patching and vulnerability remediation requirements.	0
Malware	Malware & Threat Protection	Anti-malware controls, endpoint protection, and threat monitoring.	0
BCP	Business Continuity	Backup, disaster recovery, and business continuity planning.	0
Incident Rpt	Logging & Audit Trail	Log retention (180 days), synchronized clocks, and audit trails.	1

Critical Severity Findings

1

Apache HTTP Server < 2.4.60 Multiple Vulnerabilities - Linux

CVSS 9.8

HOST 203.0.113.45 **PORT** 80/
tcp **FAMILY** Web
Servers

DESCRIPTION

Installed version: 2.4.58
Fixed version: 2.4.60
Installation
path / port: 80/tcp

REMEDIATION

Update to version 2.4.60 or later.

CVE-2024-36387

CVE-2024-38473

CVE-2024-38474

CVE-2024-38475

CVE-2024-38476

CVE-2024-38477

CVE-2024-39573

High Severity Findings

3

OpenBSD OpenSSH < 4.4p1, 8.5p1 - 9.7p1 RCE Vulnerability (regreSSHion)

CVSS 8.1

HOST 203.0.113.45 **PORT** 22/
tcp **FAMILY** General

DESCRIPTION

Installed version: 9.6p1
Fixed version: 9.8
Installation
path / port: 22/tcp

REMEDIATION

Update to version 9.8 or later.

CVE-2024-6387

CERT-In Access Control

Apache HTTP Server < 2.4.59 Multiple Vulnerabilities - Linux

CVSS 7.5

HOST 203.0.113.45 **PORT** 80/
tcp **FAMILY** Web
Servers

DESCRIPTION

Installed version: 2.4.58

Fixed version: 2.4.59

Installation

path / port: 80/tcp

REMEDIATION

Update to version 2.4.59 or later.

CVE-2023-38709

CVE-2024-24795

CVE-2024-27316

Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSH, D(HE)ater)

CVSS 7.5

HOST 203.0.113.45 **PORT** 22/
tcp **FAMILY** SSL and
TLS

DESCRIPTION

The remote SSH server supports the following DHE KEX algorithm(s):

diffie-hellman-group14-sha256

diffie-hellman-group16-sha512

diffie-hellman-group18-sha512

diffie-hellman-group-exchange-sha256

REMEDIATION

- DHE key exchange should be disabled if no other mitigation mechanism can be used and either elliptic-curve variant of Diffie-Hellman (ECDHE) or RSA key exchange is supported by the clients. The fact that RSA key exchange is not forward secret should be considered.
- Limit the maximum number of concurrent connections in e.g. the configuration of the remote server. For OpenSSH this limit can be configured via the 'MaxStartups' option, for other products please refer to the manual of the product in question on configuration possibilities.

CVE-2002-20001

CVE-2022-40735

CVE-2024-41996

CERT-In Access Control

Medium Severity Findings

11

OpenBSD OpenSSH 6.8p1 - 9.9p1 MitM Vulnerability

CVSS 6.8

HOST 203.0.113.45 **PORT** 22/
tcp **FAMILY** General

DESCRIPTION

Installed version: 9.6p1

Fixed version: 9.9p2

Installation

path / port: 22/tcp

REMEDIATION

Update to version 9.9p2 or later.

[CVE-2025-26465](#)

[CERT-In Access Control](#)

OpenBSD OpenSSH 9.5p1 - 9.9p1 DoS Vulnerability

CVSS 5.9

HOST 203.0.113.45 **PORT** 22/
tcp **FAMILY** Denial of
Service

DESCRIPTION

Installed version: 9.6p1

Fixed version: 9.9p2

Installation

path / port: 22/tcp

REMEDIATION

Update to version 9.9p2 or later.

[CVE-2025-26466](#)

[CERT-In Access Control](#)

Prefix Truncation Attacks in SSH Specification (Terrapin Attack)

CVSS 5.9

HOST 203.0.113.45

PORT 22/
tcp

FAMILY General

DESCRIPTION

The remote SSH server supports the following possible affected client-to-server encryption algorithm(s):

chacha20-poly1305@openssh.com

The remote SSH server supports the following possible affected server-to-client encryption algorithm(s):

chacha20-poly1305@openssh.com

The remote SSH server supports the following "strict kex" algorithm as a possible mitigation:

kex-strict-s-v00@openssh.com

REMEDIATION

- Update OpenSSH to version 9.6 or later
- Update Apache MINA SSHD to version 2.12.0 or later
- For other products please contact the vendor for possible fixes / updates

Mitigation:

- To mitigate this protocol vulnerability, OpenSSH suggested a so-called 'strict kex' which alters the SSH handshake to ensure a Man-in-the-Middle attacker cannot introduce unauthenticated messages as well as convey sequence number manipulation across handshakes. Support for strict key exchange has been added to a variety of SSH implementations, including OpenSSH itself, PuTTY, libssh, and more.

Warning: To take effect, both the client and server must support this countermeasure.

As a stop-gap measure, peers may also (temporarily) disable the affected algorithms and use unaffected alternatives like AES-GCM instead until patches are available.

CVE-2023-48795

CVE-2024-41909

CERT-In Access Control

Apache HTTP Server 2.4.7 - 2.4.65 Authentication Bypass Vulnerability - Linux

CVSS 5.8

HOST 203.0.113.45 **PORT** 80/
tcp **FAMILY** Web
Servers

DESCRIPTION

Installed version: 2.4.58

Fixed version: 2.4.66

Installation

path / port: 80/tcp

REMEDIATION

Update to version 2.4.66 or later.

[CVE-2025-66200](#)

OpenSSH Information Disclosure Vulnerability (CVE-2016-20012)

CVSS 5.3

HOST 203.0.113.45 **PORT** 22/
tcp **FAMILY** General

DESCRIPTION

Installed version: 9.6p1

Fixed version: None

Installation

path / port: 22/tcp

REMEDIATION

No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

[CVE-2016-20012](#)

[CERT-In Access Control](#)

Apache HTTP Server 2.4.17 < 2.4.64 DoS Vulnerability - Linux

CVSS 5.0

HOST 203.0.113.45 **PORT** 80/
tcp **FAMILY** Web
Servers

DESCRIPTION

Installed version: 2.4.58

Fixed version: 2.4.64

Installation

path / port: 80/tcp

REMEDIATION

Update to version 2.4.64 or later.

[CVE-2025-53020](#)

Apache HTTP Server 2.4.26 < 2.4.64 DoS Vulnerability - Linux

CVSS 5.0

HOST 203.0.113.45 **PORT** 80/
tcp **FAMILY** Web
Servers

DESCRIPTION

Installed version: 2.4.58

Fixed version: 2.4.64

Installation

path / port: 80/tcp

REMEDIATION

Update to version 2.4.64 or later.

[CVE-2025-49630](#)

Apache HTTP Server 2.4.35 < 2.4.64 Access Control Bypass Vulnerability - Linux

CVSS 5.0

HOST 203.0.113.45 **PORT** 80/
tcp **FAMILY** Web
Servers

DESCRIPTION

Installed version: 2.4.58

Fixed version: 2.4.64

Installation

path / port: 80/tcp

REMEDIATION

Update to version 2.4.64 or later.

[CVE-2025-23048](#)

Apache HTTP Server < 2.4.64 Multiple Vulnerabilities - Linux

CVSS 5.0

HOST 203.0.113.45 **PORT** 80/
tcp **FAMILY** Web
Servers

DESCRIPTION

Installed version: 2.4.58

Fixed version: 2.4.64

Installation

path / port: 80/tcp

REMEDIATION

Update to version 2.4.64 or later.

[CVE-2024-42516](#)

[CVE-2024-43204](#)

[CVE-2024-47252](#)

[CVE-2025-49812](#)

Apache HTTP Server 2.4.x < 2.4.66 Improper Neutralization Vulnerability - Linux

CVSS 4.3

HOST 203.0.113.45 **PORT** 80/
tcp **FAMILY** Web
Servers

DESCRIPTION

Installed version: 2.4.58

Fixed version: 2.4.66

Installation

path / port: 80/tcp

REMEDIATION

Update to version 2.4.66 or later.

[CVE-2025-65082](#)

Apache HTTP Server < 2.4.66 SSI Vulnerability - Linux

CVSS 4.3

HOST 203.0.113.45 **PORT** 80/
tcp **FAMILY** Web
Servers

DESCRIPTION

Installed version: 2.4.58

Fixed version: 2.4.66

Installation

path / port: 80/tcp

REMEDIATION

Update to version 2.4.66 or later.

[CVE-2025-58098](#)

Low Severity Findings

7

OpenBSD OpenSSH 7.4 - 9.9 Unspecified Vulnerability

CVSS 3.8

HOST 203.0.113.45 **PORT** 22/
tcp **FAMILY** General

DESCRIPTION

Installed version: 9.6p1
Fixed version: 10.0
Installation
path / port: 22/tcp

REMEDIATION

Update to version 10.0 or later.

[CVE-2025-32728](#)

[CERT-In Access Control](#)

OpenBSD OpenSSH 9.5p1 - 9.7p1 Information Disclosure Vulnerability

CVSS 3.3

HOST 203.0.113.45 **PORT** 22/
tcp **FAMILY** General

DESCRIPTION

Installed version: 9.6p1
Fixed version: 9.8
Installation
path / port: 22/tcp

REMEDIATION

Update to version 9.8 or later.

[CVE-2024-39894](#)

[CERT-In Access Control](#)

Apache HTTP Server 2.4.30 - 2.4.65 Integer Overflow Vulnerability - Linux

CVSS 2.6

HOST 203.0.113.45 **PORT** 80/
tcp **FAMILY** Web
Servers

DESCRIPTION

Installed version: 2.4.58
Fixed version: 2.4.66
Installation
path / port: 80/tcp

REMEDIATION

Update to version 2.4.66 or later.

[CVE-2025-55753](#)

TCP Timestamps Information Disclosure

CVSS 2.6

HOST 203.0.113.45 **PORT** general/
tcp **FAMILY** General

DESCRIPTION

It was detected that the host implements RFC1323/RFC7323.

The following timestamps were retrieved with a delay of 1 seconds in-between:

Packet 1: 2823216797

Packet 2: 2823217825

REMEDIATION

To disable TCP timestamps on linux add the line
'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.

To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'

Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.

The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.

See the references for more information.

Weak MAC Algorithm(s) Supported (SSH)

CVSS 2.6

HOST 203.0.113.45 **PORT** 22/
tcp **FAMILY** SSL and
TLS

DESCRIPTION

The remote SSH server supports the following weak client-to-server MAC algorithm(s):

umac-64-etm@openssh.com

umac-64@openssh.com

The remote SSH server supports the following weak server-to-client MAC algorithm(s):

umac-64-etm@openssh.com

umac-64@openssh.com

REMEDIATION

Disable the reported weak MAC algorithm(s).

CERT-In Access Control

OpenBSD OpenSSH < 10.1 Multiple Vulnerabilities

CVSS 2.4

HOST 203.0.113.45 **PORT** 22/
tcp **FAMILY** General

DESCRIPTION

Installed version: 9.6p1

Fixed version: 10.1

Installation

path / port: 22/tcp

REMEDIATION

Update to version 10.1 or later.

[CVE-2025-61984](#)

[CVE-2025-61985](#)

[CERT-In Access Control](#)

ICMP Timestamp Reply Information Disclosure

CVSS 2.1

HOST 203.0.113.45 **PORT** general/
icmp **FAMILY** General

DESCRIPTION

The following response / ICMP packet has been received:

- ICMP Type: 14

- ICMP Code: 0

REMEDIATION

Various mitigations are possible:

- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

[CVE-1999-0524](#)

Informational Findings

40 items — no remediation required

FINDING	HOST	PORT	FAMILY
Allowed HTTP Methods Enumeration	203.0.113.45	80/tcp	Web Servers
Apache HTTP Server Detection Consolidation	203.0.113.45	general/tcp	Product detection
CPE Inventory	203.0.113.45	general/CPE-T	Service detection
HTTP Security Headers Detection	203.0.113.45	80/tcp	Web application abuses
HTTP Server Banner Enumeration	203.0.113.45	80/tcp	Service detection
HTTP Server type and version	203.0.113.45	80/tcp	Service detection
Hostname Determination Reporting	203.0.113.45	general/tcp	Service detection
OS Detection Consolidation and Reporting	203.0.113.45	general/tcp	Product detection
Obtain list of all port mapper registered programs via RPC	203.0.113.45	111/tcp	Service detection
OpenSSH Detection Consolidation	203.0.113.45	general/tcp	Product detection
PQC Key Exchange (KEX) Algorithm(s) Supported (SSH)	203.0.113.45	22/tcp	SSL and TLS
RPC Portmapper Service Detection (TCP)	203.0.113.45	111/tcp	Service detection
SSH Protocol Algorithms Supported	203.0.113.45	22/tcp	Service detection
SSH Protocol Versions Supported	203.0.113.45	22/tcp	Service detection
SSH Server type and version	203.0.113.45	22/tcp	Product detection
Services	203.0.113.45	22/tcp	Service detection
Services	203.0.113.45	80/tcp	Service detection
Traceroute	203.0.113.45	general/tcp	General
Unknown	—	—	—
Unknown	—	—	—
Unknown	—	—	—
Unknown	—	—	—
Unknown	—	—	—
Unknown	—	—	—
Unknown	—	—	—
Unknown	—	—	—
Unknown	—	—	—
Unknown	—	—	—
Unknown	—	—	—
Unknown	—	—	—
Unknown	—	—	—
Unknown	—	—	—

FINDING	HOST	PORT	FAMILY
Unknown	—	—	—
Unknown	—	—	—
Unknown	—	—	—
Unknown	—	—	—
Unknown	—	—	—
Unknown	—	—	—
Unknown	—	—	—
Web Application Scanning Consolidation / Info Reporting	203.0.113.45	80/tcp	Web application abuses