

CVE-2017-7494

Samba Remote Code Execution Vulnerability

Exigent

CISA KEV since Mar 30, 2023

Actively exploited

Ransomware use known

Public exploit module (Metasploit)

Samba since version 3.5.0 and before 4.6.4, 4.5.10 and 4.4.14 is vulnerable to remote code execution vulnerability, allowing a malicious client to upload a shared library to a writable share, and then cause the server to load and execute it.

EVRS

94/100

Immediate priority

CVSS V3.1

9.8

Critical · NVD

EPSS

0.994

99.94th percentile · FIRST

CISA DEADLINE

Apr 20, 2023

KEV since 2023 · listed over a year

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☒ Ransomware	Known ransomware campaigns	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.994 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified**CISA required action:** Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
samba	$\geq 3.5.0 < 4.4.0$ $\geq 4.4.0 < 4.4.14$ $\geq 4.5.0 < 4.5.10$ $\geq 4.6.0 < 4.6.4$	no fixed version listed	NVD
debian linux	8.0	no fixed version listed	NVD

Sources

Vendor guidance	samba.org/samba/security/CVE-2017-7494.html	NVD	nvd.nist.gov/vuln/detail/CVE-2017-7494
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2017-16511
Current data	evulnable.com/vulnerability-management/cve/CVE-2017-7494		

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.