

CVE-2023-47246

SysAid Server Path Traversal Vulnerability

Exigent

CISA KEV since Nov 13, 2023

Actively exploited

Ransomware use known

In SysAid On-Premise before 23.3.36, a path traversal vulnerability leads to code execution after an attacker writes a file to the Tomcat webroot, as exploited in the wild in November 2023.

EVRS 93/100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.989 99.93rd percentile · FIRST	CISA DEADLINE Dec 4, 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	0.989 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 mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
sysaid	< 23.3.36	23.3.36	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-w3gp-79x2-f8rp	Additional guidance	documentation.sysaid.com/docs/on-premise-security-enhancements-2023
sysaid.com	sysaid.com/blog/service-desk/on-premise-software-security-vulnerability-notification	NVD	nvd.nist.gov/vuln/detail/CVE-2023-47246
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2023-51378
Current data	evulnable.com/vulnerability-management/cve/CVE-2023-47246		

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