

CVE-2024-57726

SimpleHelp Missing Authorization Vulnerability

Exigent

CISA KEV since Apr 24, 2026

Actively exploited

Ransomware use known

SimpleHelp remote support software v5.5.7 and before has a vulnerability that allows low-privileges technicians to create API keys with excessive permissions. These API keys can be used to escalate privileges to the server admin role.

EVRS 88/100 Immediate priority	CVSS V3.1 9.9 Critical · NVD	EPSS 0.664 99.28th percentile · FIRST	CISA DEADLINE May 8, 2026 CISA federal deadline · Overdue by 5 months
--	--	---	---

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	Added to CISA KEV within the last year
☒ EPSS	0.664 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.9	☐ 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, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
simplehelp	< 5.5.8	5.5.8	NVD

Sources

Vendor guidance github.com/advisories/GHSA-8388-c89m-3x67

simple-help.com simple-help.com/kb---security-vulnerabilities-01-2025#security-vulnerabilities-in-simplehelp-5-5-7-and-earlier

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

Current data evulnable.com/vulnerability-management/cve/CVE-2024-57726

NVD nvd.nist.gov/vuln/detail/CVE-2024-57726

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2024-53724

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