

CVE-2025-14611

Gladinet CentreStack and Triofox Hard Coded Cryptographic Vulnerability

CISA KEV since Dec 15, 2025

Actively exploited

Public exploit module (Metasploit)

Gladinet CentreStack and Triofox prior to version 16.12.10420.56791 used hardcoded values for their implementation of the AES cryptoscheme. This degrades security for public exposed endpoints that may make use of it and may offer arbitrary local file inclusion when provided a specially crafted request without authentication. This opens the door for future exploitation and can be leveraged with previous vulnerabilities to gain a full system compromise.

EVRS 75/₁₀₀ Urgent priority	CVSS V4.0 7.1 High · NVD	EPSS 0.533 99th percentile · FIRST	CISA DEADLINE Jan 5, 2026 CISA federal deadline · Overdue by 10 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	No known ransomware campaign association	☐ KEV recency	Added to CISA KEV within the last year
☒ EPSS	0.533 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.1	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle 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
centrestack	< 16.12.10420.56791	16.12.10420.56791	NVD
triofox	< 16.12.10420.56791	16.12.10420.56791	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-j7r7-3wrm-f59w	centrestack.com	centrestack.com/p/gce_latest_release.html
access.triofox.com	access.triofox.com/releases_history/	support.centrestack.com	support.centrestack.com/hc/en-us/articles/360007159054-Hardening-the-CentreStack-Cluster#h_01JQRV57T37HJFQZKBZH9NBXQP
NVD	nvd.nist.gov/vuln/detail/CVE-2025-14611	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2025-203165	Current data	evulnabile.com/vulnerability-management/cve/CVE-2025-14611

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