

CVE-2019-6693

Fortinet FortiOS Use of Hard-Coded Credentials Vulnerability

CISA KEV since Jun 25, 2025

Actively exploited

Ransomware use known

Use of a hard-coded cryptographic key to cipher sensitive data in FortiOS configuration backup file may allow an attacker with access to the backup file to decipher the sensitive data, via knowledge of the hard-coded key. The aforementioned sensitive data includes users' passwords (except the administrator's password), private keys' passphrases and High Availability password (when set).

EVRS 75/₁₀₀ Urgent priority	CVSS V3.1 6.5 Medium · NVD	EPSS 0.066 93.9th percentile · FIRST	CISA DEADLINE Jul 16, 2025 KEV since 2025 · 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	Added to CISA KEV within the last two years
☒ EPSS	0.066 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 6.5	☐ 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
fortios	$\leq 5.6.10$ $\geq 6.0.0 \leq 6.0.6$ $6.2.0$	after 5.6.10 · after 6.0.6	NVD

Sources

Vendor guidance	fortiguard.com/advisory/FG-IR-19-007	NVD	nvd.nist.gov/vuln/detail/CVE-2019-6693
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2019-16251
Current data	evulnable.com/vulnerability-management/cve/CVE-2019-6693		

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