

CVE-2019-5591

Fortinet FortiOS Default Configuration Vulnerability

CISA KEV since Nov 3, 2021

Actively exploited

Ransomware use known

A Default Configuration vulnerability in FortiOS may allow an unauthenticated attacker on the same subnet to intercept sensitive information by impersonating the LDAP server.

EVRS 75 / ₁₀₀ Urgent priority	CVSS V3.1 6.5 Medium · NVD	EPSS 0.186 97.3rd percentile · FIRST	CISA DEADLINE May 3, 2022 KEV since 2021 · 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	0.186 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 updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
fortios	≤ 6.2.0	after 6.2.0	NVD

Sources

Vendor guidance	fortiguard.com/psirt/FG-IR-19-037	NVD	nvd.nist.gov/vuln/detail/CVE-2019-5591
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2019-15166
Current data	evulnable.com/vulnerability-management/cve/CVE-2019-5591		

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