

CVE-2018-13379

Fortinet FortiOS SSL VPN Path Traversal Vulnerability

Exigent

CISA KEV since Nov 3, 2021

Actively exploited

Ransomware use known

Public exploit module (Metasploit)

An Improper Limitation of a Pathname to a Restricted Directory ("Path Traversal") in Fortinet FortiOS 6.0.0 to 6.0.4, 5.6.3 to 5.6.7 and 5.4.6 to 5.4.12 and FortiProxy 2.0.0, 1.2.0 to 1.2.8, 1.1.0 to 1.1.6, 1.0.0 to 1.0.7 under SSL VPN web portal allows an unauthenticated attacker to download system files via special crafted HTTP resource requests.

EVRs

94/100

Immediate priority

CVSS V3.1

9.8

Critical · NVD

EPSS

0.999

99.99th 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	0.999 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 updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
fortiproxy	< 1.2.9 2.0.0	1.2.9	NVD
fortios	≥ 5.4.6 < 5.4.13 ≥ 5.6.3 < 5.6.8 ≥ 6.0.0 < 6.0.5	5.4.13 · 5.6.8 · 6.0.5	NVD

Sources

Vendor guidance	fortiguard.com/advisory/FG-IR-18-384	NVD	nvd.nist.gov/vuln/detail/CVE-2018-13379
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2018-5323
Current data	evulnable.com/vulnerability-management/cve/CVE-2018-13379		

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