CVE-2018-13382

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2018-13382
State	PUBLIC
Assigner	psirt@fortinet.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-06-04 21:29:00 UTC
Updated	2021-06-03 11:15:00 UTC
Description	An Improper Authorization vulnerability in Fortinet FortiOS 6.0.0 to 6.0.4, 5.6.0 to 5.6.8 and 5.4.1 to 5.4.10 and FortiProxy 2

Risk And Classification

EPSS: 0.870820000 probability, percentile 0.994500000 (date 2026-05-08)

CISA KEV: Listed on 2022-01-10; due 2022-07-10; ransomware use Known

Problem Types: CWE-285

CISA Known Exploited Vulnerability

Vendor	Fortinet
Product	FortiOS and FortiProxy
Name	Fortinet FortiOS and FortiProxy Improper Authorization
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2018-13382

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fortinet	Fortios	All	All	All	All
Operating System	Fortinet	Fortios	All	All	All	All
Operating System	Fortinet	Fortios	All	All	All	All

References

Reference	Source	Link	Tags
Fortinet FortiOS CVE-2018-13382 Authorization Bypass Vulnerability	BID	www.securityfocus.com	
Unauthenticated SSL VPN users password modification | FortiGuard	CONFIRM	fortiguard.com	Mitigation, Vendo

Attacking SSL VPN - Part 2: Breaking the Fortigate SSL VPN | DEVCORE	MISC	devco.re	
Fortinet FortiOS 6.0.4 Password Modification ≈ Packet Storm	MISC	packetstormsecurity.com	
FortiProxy - Unauthenticated SSL VPN users password modification | FortiGuard	CONFIRM	www.fortiguard.com	
i.blackhat.com/USA-19/Wednesday/us-19-Tsai-Infiltrating-Corporate-Intranet-L...	MISC	i.blackhat.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analys
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov	kev

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.