CVE-2018-13379

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

Summary

CVE	CVE-2018-13379
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 Limitation of a Pathname to a Restricted Directory ("Path Traversal") in Fortinet FortiOS 6.0.0 to 6.0.4, 5.6.3 to

Risk And Classification

EPSS: 0.944730000 probability, percentile 0.999990000 (date 2026-05-08)

CISA KEV: Listed on 2021-11-03; due 2022-05-03; ransomware use Known

Problem Types: CWE-22

CISA Known Exploited Vulnerability

Vendor	Fortinet
Product	FortiOS
Name	Fortinet FortiOS SSL VPN Path Traversal Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2018-13379

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

References

Reference	Source	Link
FortiOS 5.6.7 / 6.0.4 Credential Disclosure ≈ Packet Storm	MISC	pack
Attacking SSL VPN - Part 2: Breaking the Fortigate SSL VPN | DEVCORE	MISC	devc
i.blackhat.com/USA-19/Wednesday/us-19-Tsai-Infiltrating-Corporate-Intranet-L...	MISC	i.bla

FortiProxy - system file leak through SSL VPN special crafted HTTP resource requests | FortiGuard	CONFIRM	www
Development/CVE-2018-13379 - Summary & Emergency Mitigations.pdf at master · blacklotuslabs/Development · GitHub	MISC	gith
Fortinet FortiOS CVE-2018-13379 Directory Traversal Vulnerability	BID	www
FortiOS system file leak through SSL VPN via specially crafted HTTP resource requests | FortiGuard	CONFIRM	forti
FortiOS 5.6.7 / 6.0.4 Credential Disclosure ≈ Packet Storm	MISC	pacl
CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd.
CISA Known Exploited Vulnerabilities catalog	CISA	www

No vendor comments have been submitted for this CVE.

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