



CVE-2019-5587

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2019-5587
State	PUBLIC
Assigner	psirt@fortinet.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-06-04 22:29:00 UTC
Updated	2022-04-22 20:11:00 UTC
Description	Lack of root file system integrity checking in Fortinet FortiOS VM application images all versions below 6.0.5 may allow atta

Risk And Classification

Problem Types: CWE-345

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	Tags
VM images lack an integrity check of the file system at boot time FortiGuard	CONFIRM	fortiguard.com	Vendor Advisory
Fortinet FortiOS VM CVE-2019-5587 Local Security Bypass Vulnerability	BID	www.securityfocus.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report