



CVE-2021-32603

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

Summary

CVE	CVE-2021-32603
State	PUBLIC
Assigner	psirt@fortinet.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-08-05 11:15:00 UTC
Updated	2021-08-12 19:32:00 UTC
Description	A server-side request forgery (SSRF) (CWE-918) vulnerability in FortiManager and FortiAnalyser GUI 7.0.0, 6.4.5 and below

Risk And Classification

Problem Types: CWE-918

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Fortinet	Fortianalyzer	All	All	All	All
Application	Fortinet	Fortimanager	All	All	All	All

References

Reference	Source	Link	Tags
FortiManager & FortiAnalyzer - Improper validation of dispatcher socket parameters FortiGuard	CONFIRM	fortiguard.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ar

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[376129](#) FortiGate FortiManager and FortiAnalyzer Server-Side Request Forgery (SSRF) Vulnerability (CWE-918)

consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This 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](#).

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