CVE-2021-24020

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-24020
State	PUBLIC
Assigner	psirt@fortinet.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-07-09 19:15:00 UTC
Updated	2022-07-12 17:42:00 UTC
Description	A missing cryptographic step in the implementation of the hash digest algorithm in FortiMail 6.4.0 through 6.4.4, and 6.2.0 t

Risk And Classification

Problem Types: CWE-347

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Fortinet	Fortimail	All	All	All	All
Application	Fortinet	Fortimail	All	All	All	All

References

Reference	Source	Link	Tags
FortiMail - Salted Digest vulnerable to length extension attacks | FortiGuard	CONFIRM	fortiguard.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.

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