



# CVE-2021-26095

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

## Summary

<b>CVE</b>	CVE-2021-26095
<b>State</b>	PUBLIC
<b>Assigner</b>	psirt@fortinet.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-07-20 11:15:00 UTC
<b>Updated</b>	2023-08-08 14:22:00 UTC
<b>Description</b>	The combination of various cryptographic issues in the session management of FortiMail 6.4.0 through 6.4.4 and 6.2.0 thro

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## 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	Ta
FortiMail - Improper cryptographic operations in cookie encryption potentially prone to forgery   FortiGuard	CONFIRM	<a href="https://fortiguard.com">fortiguard.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	ca
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	ca

No vendor comments have been submitted for this CVE.

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

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](#)**