



CVE-2021-32094

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

Summary

CVE	CVE-2021-32094
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-05-07 04:15:00 UTC
Updated	2021-05-12 21:02:00 UTC
Description	U.S. National Security Agency (NSA) Emissary 5.9.0 allows an authenticated user to upload arbitrary files.

Risk And Classification

Problem Types: CWE-434

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nsa	Emissary	5.9.0	All	All	All

References

Reference	Source	Link	Tags
SonarSource Blog	MISC	blog.sonarsource.com	
NSA workflow application Emissary vulnerable to malicious takeover The Daily Swig	MISC	portswigger.net	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, anal

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](#)