



CVE-2021-32639

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

Summary

CVE	CVE-2021-32639
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-07-02 16:15:00 UTC
Updated	2021-07-06 18:19:00 UTC
Description	Emissary is a P2P-based, data-driven workflow engine. Emissary version 6.4.0 is vulnerable to Server-Side Request Forge

Risk And Classification

Problem Types: CWE-918

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Sou
emissary/AddChildDirectoryAction.java at 30c54ef16c6eb6ed09604a929939fb9f66868382 · NationalSecurityAgency/emissary · GitHub	MIS
emissary/RegisterPeerAction.java at 30c54ef16c6eb6ed09604a929939fb9f66868382 · NationalSecurityAgency/emissary · GitHub	MIS
Server-Side Request Forgery (SSRF) in emissary:emissary · Advisory · NationalSecurityAgency/emissary · GitHub	COM
CVE Program record	CVE
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

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](#)