CVE-2021-24040

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-24040
State	PUBLIC
Assigner	cve-assign@fb.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-09-10 22:15:00 UTC
Updated	2021-09-24 03:06:00 UTC
Description	Due to use of unsafe YAML deserialization logic, an attacker with the ability to modify local YAML configuration files could p

Risk And Classification

Problem Types: CWE-502

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Facebook	Parlai	All	All	All	All

References

Reference	Source	Link	Tags
Deserialization of Untrusted Data in parlai · Advisory · facebookresearch/ParlAI · GitHub	CONFIRM	github.com	
Facebook ParlAI 1.0.0 Code Execution / Deserialization ≈ Packet Storm	MISC	packetstormsecurity.com	
Release v1.1.0 · facebookresearch/ParlAI · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical,

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

980998 Python (pip) Security Update for parlai (GHSA-mwgj-7x7j-6966)

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