



CVE-2018-3972

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

Summary

CVE	CVE-2018-3972
State	PUBLIC
Assigner	talos-cna@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-09-26 12:29:00 UTC
Updated	2023-02-02 13:39:00 UTC
Description	An exploitable code execution vulnerability exists in the Levin deserialization functionality of the Epee library, as used in Mo

Risk And Classification

Problem Types: CWE-502

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Getmonero	Monero	0.12.2.0	All	All	All
Application	Getmonero	Monero	0.12.2.0	All	All	All

References

Reference

TALOS-2018-0637 Cisco Talos Intelligence Group - Comprehensive Threat Intelligence
Cisco Talos Intelligence Group - Comprehensive Threat Intelligence: Vulnerability Spotlight: Epee Levin Packet Deserialization Code Execution
CVE Program record
NVD vulnerability detail

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](#).

Free CVE JSON API cve.report/api

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