



CVE-2022-29528

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2022-29528
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-04-20 23:15:00 UTC
Updated	2023-12-21 03:15:00 UTC
Description	An issue was discovered in MISP before 2.4.158. PHAR deserialization can occur.

Risk And Classification

Problem Types: CWE-502

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Misp	Misp	All	All	All	All

References

Reference

- MISP - PHAR deserialization | Web Application Security Testing
- Comparing v2.4.157...v2.4.158 · MISP/MISP · GitHub
- CakePHP Application Cybersecurity Research - Exploring the PHAR Deserialization PHP Vulnerability: A White Box Testing Example | Web A
- fix: [security] Sanitise paths for several file interactions · MISP/MISP@93821c0 · GitHub
- fix: [security] unregister phar from stream wrappers globally for all... · MISP/MISP@0108f1b · GitHub
- 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.

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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