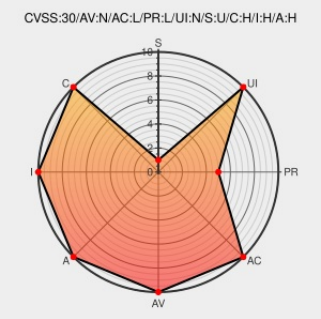
CVE-2018-19908

Published on: 12/06/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:40 PM UTC

CVE-2018-19908

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Misp from Misp contain the following vulnerability:

An issue was discovered in MISP 2.4.9x before 2.4.99. In app/Model/Event.php (the STIX 1 import code), an unescaped filename string is used to construct a shell command. This vulnerability can be abused by a malicious authenticated user to execute arbitrary commands by tweaking the original filename of the STIX import.

CVE-2018-19908 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 9 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
fix: [internal] Handle the upload of original versions of ingested fi… · MISP/MISP@211ac07 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/MISP/MISP/commit/211ac0737281b65e7da160f0aac52f401a94e1a3

Release MISP 2.4.99 released (aka API/UI fixes and critical security vulnerability fixed) · MISP/MISP · GitHub	Release Notes Third Party Advisory github.com text/html	MISC github.com/MISP/MISP/releases/tag/v2.4.99
MISP 2.4.97 - SQL Command Execution via Command Injection in STIX Module - PHP webapps Exploit	Exploit Third Party Advisory VDB Entry www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 46401

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:misp:misp:*:*:*:*:*:*:*:*:

cpe:2.3:a:misp:misp:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→