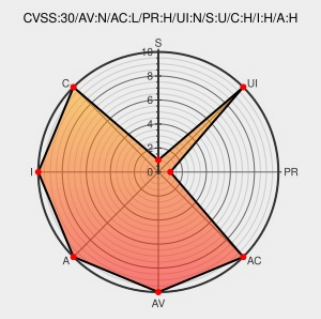
CVE-2018-6926

Published on: 02/12/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:47 PM UTC

CVE-2018-6926

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



Certain versions of Misp from Misp contain the following vulnerability:

In app/Controller/ServersController.php in MISP 2.4.87, a server setting permitted the override of a path variable on certain Red Hed Enterprise Linux and CentOS systems (where rh_shell_fix was enabled), and consequently allowed site admins to inject arbitrary OS commands. The impact is limited by the setting being only accessible to the site administrator.

CVE-2018-6926 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.2 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	HIGH	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: Fixed command execution for site admins · MISP/MISP@0a2aa9d · GitHub	Patch Third Party Advisory github.com	CONFIRM github.com/MISP/MISP/commit/0a2aa9d52492d960b9a161160acedbe9caaa4126

text/html

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	2.4.87	All	All	All
Application	Misp	Misp	2.4.87	All	All	All

cpe:2.3:a:misp:misp:2.4.87:*:*:*:*:*:*:*:

cpe:2.3:a:misp:misp:2.4.87:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→