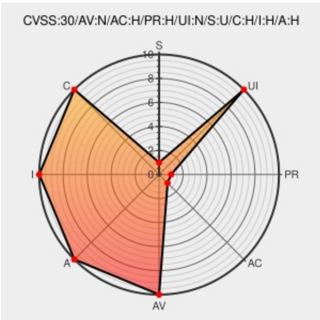
CVE-2019-12794

Published on: 06/11/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:40 PM UTC

CVE-2019-12794

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



Certain versions of Misp from Misp contain the following vulnerability:

An issue was discovered in MISP 2.4.108. Organization admins could reset credentials for site admins (organization admins have the inherent ability to reset passwords for all of their organization's users). This, however, could be abused in a situation where the host organization of an instance creates organization admins. An organization admin could set a password manually for the site admin or simply use the API key of the site admin to impersonate them. The potential for abuse only occurs when the host organization creates lower-privilege organization admins instead of the usual site admins. Also, only organization admins of the same organization as the site admin could abuse this.

CVE-2019-12794 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.6 - MEDIUM

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

CVSS2 Score: 6 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
fix: [security] Org admins could reset credentials for site admins · MISP/MISP@36b43f1 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/MISP/MISP/commit/36b43f1306873cff87b7aa30cdc1a30b38c9c16a

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	2.4.108	All	All	All
Application	Misp	Misp	2.4.108	All	All	All

cpe:2.3:a:misp:misp:2.4.108:*:*:*:*:*:*:*:

cpe:2.3:a:misp:misp:2.4.108:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→