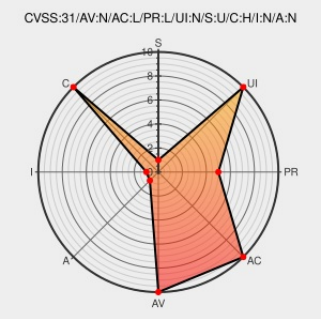
CVE-2019-16202

Published on: 09/10/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:49 PM UTC

CVE-2019-16202

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



Certain versions of Misp from Misp contain the following vulnerability:

MISP before 2.4.115 allows privilege escalation in certain situations. After updating to 2.4.115, escalation attempts are blocked by the __checkLoggedActions function with a "This could be an indication of an attempted privilege escalation on older vulnerable versions of MISP (<2.4.115)" message.

CVE-2019-16202 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.5 - MEDIUM

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

CVSS2 Score: 4 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
fix: [security] Fix to a vulnerability related to the server index · MISP/MISP@75acd63 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/MISP/MISP/commit/75acd63c46506ad404764c3a3de7d4ca11d0560f

CVE-2019-16202 - Excellium Services	Third Party Advisory excellium-services.com text/html	CONFIRM excellium-services.com/cert-xlm-advisory/cve-2019-16202/
Comparing v2.4.114...v2.4.115 · MISP/MISP · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/MISP/MISP/compare/v2.4.114...v2.4.115

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→