

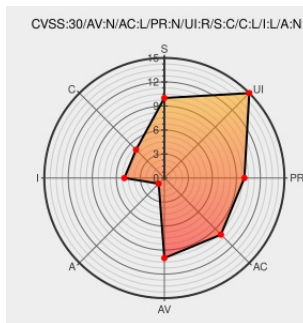


CVE-2018-14504

Published on: 08/03/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:43 PM UTC

CVE-2018-14504

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Mantisbt](#) from [Mantisbt](#) contain the following vulnerability:

An issue was discovered in `manage_filter_edit_page.php` in MantisBT 2.x through 2.15.0. A cross-site scripting (XSS) vulnerability in the Edit Filter page allows execution of arbitrary code (if CSP settings permit it) when displaying a filter with a crafted name (e.g., "foobar" `onclick="alert(1)"`).

CVE-2018-14504 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.1 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	LOW	NONE

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
0024608: CVE-2018-14504: XSS in edit filters page - MantisBT	Exploit Issue Tracking Patch MantisBT	CONFIRM mantisbt.org/bugs/view.php?id=24608

Vendor Advisory

mantisbt.org

text/html

MantisBT 2.16.0 and 2.15.1 Released – Mantis Bug Tracker – Blog

Vendor Advisory

mantisbt.org

text/html

 CONFIRM mantisbt.org/blog/archives/mantisbt/602

Patch

Third Party Advisory

github.com

text/html

Fix XSS on filter edit page (CVE-2018-14504) · mantisbt/mantisbt@8b5fa24 · GitHub

CONFIRM

github.com/mantisbt/mantisbt/commit/8b5fa243dbf04344a55fe880135ec149fc1f439f

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	Mantisbt	Mantisbt	All	All	All	All

cpe:2.3:a:mantisbt:mantisbt:*****:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→