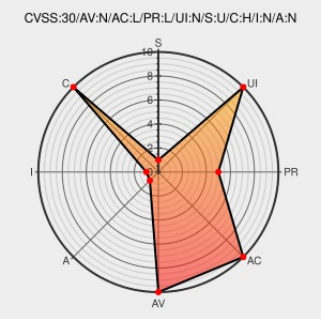
CVE-2018-9839

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

Last Modified on: 03/23/2021 11:24:54 PM UTC

CVE-2018-9839

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



Certain versions of Mantisbt from Mantisbt contain the following vulnerability:

An issue was discovered in MantisBT through 1.3.14, and 2.0.0. Using a crafted request on bug_report_page.php (modifying the 'm_id' parameter), any user with REPORTER access or above is able to view any private issue's details (summary, description, steps to reproduce, additional information) when cloning it. By checking the 'Copy issue notes' and 'Copy attachments' checkboxes and completing the clone operation, this data also becomes public (except private notes).

CVE-2018-9839 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
0024221: CVE-2018-9839:	Exploit	MISC mantisbt.org/bugs/view.php?id=24221

0024221: CVE-2018-9839: Private issues accessible to unauthorized users using the "Clone" functionality - MantisBT	Exploit Issue Tracking Third Party Advisory mantisbt.org text/html	MISC mantisbt.org/bugs/view.php?id=24221
Prevent cloning private issues by unauthorized users · mantisbt/mantisbt@1fbcd9b · GitHub	Patch Third Party Advisory github.com text/html	CONFIRM github.com/mantisbt/mantisbt/commit/1fbcd9bca2f2c77cb61624d36ddee4b3802c38ea

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	2.0.0	All	All	All
Application	Mantisbt	Mantisbt	2.0.0	All	All	All
Application	Mantisbt	Mantisbt	All	All	All	All

cpe:2.3:a:mantisbt:mantisbt:2.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:mantisbt:mantisbt:2.0.0:*:*:*:*:*:*:*:

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→