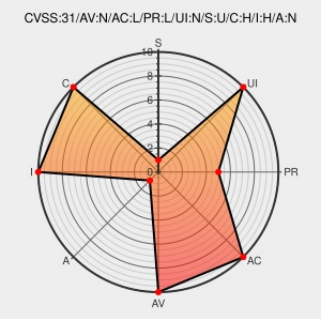
CVE-2009-20001

Published on: 03/07/2021 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:27 PM UTC

CVE-2009-20001

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



Certain versions of Mantisbt from Mantisbt contain the following vulnerability:

An issue was discovered in MantisBT before 2.24.5. It associates a unique cookie string with each user. This string is not reset upon logout (i.e., the user session is still considered valid and active), allowing an attacker who somehow gained access to a user's cookie to login as them.

CVE-2009-20001 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.1 - HIGH

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

CVSS2 Score: 5.5 - MEDIUM

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

CVE References

Description	Tags	Link
0027976: CVE-2009-20001: User cookie string is not reset upon logout - MantisBT	Exploit, Issue Tracking, Vendor Advisory	MISC mantisbt.org/bugs/view.php?id=27976

	mantisbt.org text/html	
0011296: Mantis BT is using fix cookies in the DB - MantisBT	Issue Tracking Vendor Advisory mantisbt.org text/html	MISC mantisbt.org/bugs/view.php?id=11296

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
Application	Mantisbt	Mantisbt	All	All	All	All

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→