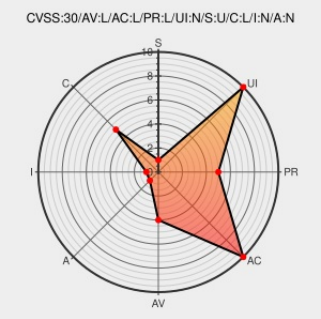
CVE-2018-6382

Published on: 01/30/2018 12:00:00 AM UTC

Last Modified on: 11/07/2023 02:59:00 AM UTC

CVE-2018-6382

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



Certain versions of Mantisbt from Mantisbt contain the following vulnerability:

** DISPUTED ** MantisBT 2.10.0 allows local users to conduct SQL Injection attacks via the vendor/adodb/adodb-php/server.php sql parameter in a request to the 127.0.0.1 IP address. NOTE: the vendor disputes the significance of this report because server.php is intended to execute arbitrary SQL statements on behalf of authenticated users from 127.0.0.1, and the issue does not have an authentication bypass.

CVE-2018-6382 has been assigned by cve@mitre.org to track the vulnerability - currently rated as LOW severity.

CVSS3 Score: 3.3 - LOW

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

CVSS2 Score: 2.1 - LOW

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

CVE References

Description	Tags	Link
No Description Provided	Vendor Advisory archive.is	MISC archive.is/https:/mantisbt.org/bugs/view.php?

	Inactive Link Not Archived	id=23908
0023908: Vendor/adodb/adodb-php/server.php SQL injection - MantisBT	Issue Tracking Vendor Advisory mantisbt.org text/html	MISC mantisbt.org/bugs/view.php?id=23908

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	2.10.0	All	All	All
Application	Mantisbt	Mantisbt	2.10.0	All	All	All

cpe:2.3:a:mantisbt:mantisbt:2.10.0:*:*:*:*:*:*:*:

cpe:2.3:a:mantisbt:mantisbt:2.10.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→