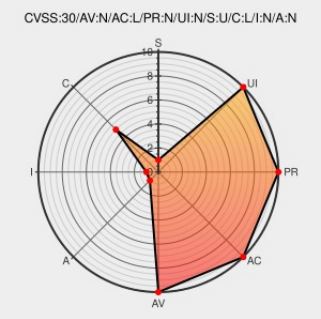
CVE-2014-9759

Published on: 04/11/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:59 PM UTC

CVE-2014-9759

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



Certain versions of Mantisbt from Mantisbt contain the following vulnerability:

Incomplete blacklist vulnerability in the config_is_private function in config_api.php in MantisBT 1.3.x before 1.3.0 allows remote attackers to obtain sensitive master salt configuration information via a SOAP API request.

CVE-2014-9759 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.3 - MEDIUM

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

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
MantisBT config_is_private() Flaw Lets Remote Users Obtain Potentially Sensitive Information on the Target System - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1035518
oss-security - Re: CVE Request: MantisBT SOAP API	www.openwall.com	MLIST [oss-security] 20160103 Re: CVE Request:

can be used to disclose confidential settings	text/html	MantisBT SOAP API can be used to disclose confidential settings
oss-security - CVE Request: MantisBT SOAP API can be used to disclose confidential settings	www.openwall.com text/html	MLIST [oss-security] 20160102 CVE Request: MantisBT SOAP API can be used to disclose confidential settings
0020277: CVE-2014-9759: SOAP API can be used to disclose confidential settings - MantisBT	Patch mantisbt.org text/html	CONFIRM mantisbt.org/bugs/view.php?id=20277
MantisBT / [mantisbt-dev] 1.3-Dev Users: Crypto_master_salt	Patch sourceforge.net text/html	CONFIRM sourceforge.net/p/mantisbt/mailman/message/32948048/

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	1.3.0	rc1	All	All
Application	Mantisbt	Mantisbt	1.3.0	rc1	All	All

cpe:2.3:a:mantisbt:mantisbt:1.3.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:mantisbt:mantisbt:1.3.0:rc1:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→