

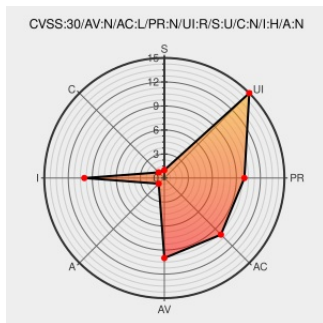


CVE-2017-7620

Published on: 05/21/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:41 PM UTC

CVE-2017-7620

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

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

MantisBT before 1.3.11, 2.x before 2.3.3, and 2.4.x before 2.4.1 omits a backslash check in string_api.php and consequently has conflicting interpretations of an initial V substring as introducing either a local pathname or a remote hostname, which leads to (1) arbitrary Permalink Injection via CSRF attacks on a permalink_page.php?url= URI and (2) an open redirect via a login_page.php?return= URI.

CVE-2017-7620 has been assigned by [M](#) 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	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	HIGH	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
	Exploit Third Party Advisory	MISC hyp3rlinx.altervista.org/advisories/MANTIS-

hyp3rlinx.altervista.org
text/plain

BUG-TRACKER-CSRF-PERMALINK-INJECTION.txt

MantisBT Input Validation Flaws Let Remote Users Conduct Cross-Site Request Forgery and Open Redirect Attacks - SecurityTracker

www.securitytracker.com
text/html

 SECTRAK 1038538

0022702: CVE-2017-7620: CSRF - Arbitrary Permalink Injection - MantisBT

Issue Tracking
mantisbt.org
text/html

 CONFIRM mantisbt.org/bugs/view.php?id=22702

Mantis Bug Tracker 1.3.10/2.3.0 - Cross-Site Request Forgery - PHP webapps Exploit

Exploit
Third Party Advisory
www.exploit-db.com
Proof of Concept
text/html

 EXPLOIT-DB 42043

0022816: CVE-2017-7620: Open redirection vulnerability in /login_page.php - MantisBT

Issue Tracking
mantisbt.org
text/html

 CONFIRM mantisbt.org/bugs/view.php?id=22816

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	2.0.0	All	All	All
Application	Mantisbt	Mantisbt	2.0.1	All	All	All
Application	Mantisbt	Mantisbt	2.1.0	All	All	All
Application	Mantisbt	Mantisbt	2.1.1	All	All	All
Application	Mantisbt	Mantisbt	2.1.2	All	All	All
Application	Mantisbt	Mantisbt	2.2.0	All	All	All
Application	Mantisbt	Mantisbt	2.2.2	All	All	All
Application	Mantisbt	Mantisbt	2.2.3	All	All	All
Application	Mantisbt	Mantisbt	2.2.4	All	All	All
Application	Mantisbt	Mantisbt	2.4.0	All	All	All
Application	Mantisbt	Mantisbt	2.0.0	All	All	All
Application	Mantisbt	Mantisbt	2.0.1	All	All	All
Application	Mantisbt	Mantisbt	2.1.0	All	All	All
Application	Mantisbt	Mantisbt	2.1.1	All	All	All
Application	Mantisbt	Mantisbt	2.1.2	All	All	All
Application	Mantisbt	Mantisbt	2.2.0	All	All	All
Application	Mantisbt	Mantisbt	2.2.2	All	All	All

Application	Mantisbt	Mantisbt	2.2.3	All	All	All
Application	Mantisbt	Mantisbt	2.2.4	All	All	All
Application	Mantisbt	Mantisbt	2.4.0	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:2.0.1:*:*:*:*:*:						
cpe:2.3:a:mantisbt:mantisbt:2.1.0:*:*:*:*:*:						
cpe:2.3:a:mantisbt:mantisbt:2.1.1:*:*:*:*:*:						
cpe:2.3:a:mantisbt:mantisbt:2.1.2:*:*:*:*:*:						
cpe:2.3:a:mantisbt:mantisbt:2.2.0:*:*:*:*:*:						
cpe:2.3:a:mantisbt:mantisbt:2.2.2:*:*:*:*:*:						
cpe:2.3:a:mantisbt:mantisbt:2.2.3:*:*:*:*:*:						
cpe:2.3:a:mantisbt:mantisbt:2.2.4:*:*:*:*:*:						
cpe:2.3:a:mantisbt:mantisbt:2.4.0:*:*:*:*:*:						
cpe:2.3:a:mantisbt:mantisbt:2.0.0:*:*:*:*:*:						
cpe:2.3:a:mantisbt:mantisbt:2.0.1:*:*:*:*:*:						
cpe:2.3:a:mantisbt:mantisbt:2.1.0:*:*:*:*:*:						
cpe:2.3:a:mantisbt:mantisbt:2.1.1:*:*:*:*:*:						
cpe:2.3:a:mantisbt:mantisbt:2.1.2:*:*:*:*:*:						
cpe:2.3:a:mantisbt:mantisbt:2.2.0:*:*:*:*:*:						
cpe:2.3:a:mantisbt:mantisbt:2.2.2:*:*:*:*:*:						
cpe:2.3:a:mantisbt:mantisbt:2.2.3:*:*:*:*:*:						
cpe:2.3:a:mantisbt:mantisbt:2.2.4:*:*:*:*:*:						
cpe:2.3:a:mantisbt:mantisbt:2.4.0:*:*:*:*:*:						
cpe:2.3:a:mantisbt:mantisbt:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)