



CVE-2017-12061

Published on: 08/01/2017 12:00:00 AM UTC

Last Modified on: 11/01/2021 02:39:00 PM UTC

CVE-2017-12061

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

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

An XSS issue was discovered in admin/install.php in MantisBT before 1.3.12 and 2.x before 2.5.2. Some variables under user control in the MantisBT installation script are not properly sanitized before being output, allowing remote attackers to inject arbitrary JavaScript code, as demonstrated by the `$f_database`, `$f_db_username`, and

`$f_admin_username` variables. This is mitigated by the fact that the admin/ folder should be deleted after installation, and also prevented by CSP.

CVE-2017-12061 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.1 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	LOW	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
MantisBT Input Validation	CVE-2017-12061	SECTRAK 100000

mantisbt input validation Flaws in '/admin/install.php' and 'manage_user_page.php' Let Remote Users Conduct Cross-Site Scripting Attacks - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	 SECURITYTRACKER 1039030
Fix XSS in install.php (CVE-2017-12061) · mantisbt/mantisbt@17f9b94 · GitHub	Patch Third Party Advisory github.com text/html	 CONFIRM github.com/mantisbt/mantisbt/commit/17f9b94f031ba93ae2a727bca0e68458ecd08ft
oss-security - Re: Advisory: XSS issues in MantisBT (CVE-2017-12061, CVE- 2017-12062)	Mailing List Third Party Advisory openwall.com text/html	 CONFIRM openwall.com/lists/oss-security/2017/08/01/2
Fix XSS in install.php (CVE-2017-12061) · mantisbt/mantisbt@c73ae3d · GitHub	Patch Third Party Advisory github.com text/html	 CONFIRM github.com/mantisbt/mantisbt/commit/c73ae3d3d4dd4681489a9e697e8ade785e27cl
oss-security - Advisory: XSS issues in MantisBT (CVE- 2017-12061, CVE-2017- 12062)	Mailing List Third Party Advisory openwall.com text/html	 CONFIRM openwall.com/lists/oss-security/2017/08/01/1
0023146: CVE-2017-12061: XSS in /admin/install.php script - MantisBT	Issue Tracking Vendor Advisory mantisbt.org text/html	 CONFIRM mantisbt.org/bugs/view.php?id=23146

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	2.0.0	beta1	All	All
Application	Mantisbt	Mantisbt	2.0.0	beta2	All	All
Application	Mantisbt	Mantisbt	2.0.0	beta3	All	All
Application	Mantisbt	Mantisbt	2.0.0	rc1	All	All
Application	Mantisbt	Mantisbt	2.0.0	rc2	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	2.1.3	All	All	All
Application	Mantisbt	Mantisbt	2.2.0	All	All	All
Application	Mantisbt	Mantisbt	2.2.1	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	2.3.0	All	All	All
Application	Mantisbt	Mantisbt	2.3.1	All	All	All
Application	Mantisbt	Mantisbt	2.3.2	All	All	All
Application	Mantisbt	Mantisbt	2.3.3	All	All	All
Application	Mantisbt	Mantisbt	2.4.0	All	All	All
Application	Mantisbt	Mantisbt	2.4.1	All	All	All
Application	Mantisbt	Mantisbt	2.4.2	All	All	All
Application	Mantisbt	Mantisbt	2.5.0	All	All	All
Application	Mantisbt	Mantisbt	2.5.1	All	All	All
Application	Mantisbt	Mantisbt	2.0.0	beta1	All	All
Application	Mantisbt	Mantisbt	2.0.0	beta2	All	All
Application	Mantisbt	Mantisbt	2.0.0	beta3	All	All
Application	Mantisbt	Mantisbt	2.0.0	rc1	All	All
Application	Mantisbt	Mantisbt	2.0.0	rc2	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	2.1.3	All	All	All
Application	Mantisbt	Mantisbt	2.2.0	All	All	All
Application	Mantisbt	Mantisbt	2.2.1	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	2.3.0	All	All	All
Application	Mantisbt	Mantisbt	2.3.1	All	All	All
Application	Mantisbt	Mantisbt	2.3.2	All	All	All
Application	Mantisbt	Mantisbt	2.3.3	All	All	All
Application	Mantisbt	Mantisbt	2.4.0	All	All	All
Application	Mantisbt	Mantisbt	2.4.1	All	All	All

Application	Mantisbt	Mantisbt	2.4.2	All	All	All
Application	Mantisbt	Mantisbt	2.5.0	All	All	All
Application	Mantisbt	Mantisbt	2.5.1	All	All	All
Application	Mantisbt	Mantisbt	All	All	All	All
cpe:2.3:a:mantisbt:mantisbt:*.*.*.*.*.*.*:						
cpe:2.3:a:mantisbt:mantisbt:2.0.0:beta1:*.*.*.*.*.*:						
cpe:2.3:a:mantisbt:mantisbt:2.0.0:beta2:*.*.*.*.*.*:						
cpe:2.3:a:mantisbt:mantisbt:2.0.0:beta3:*.*.*.*.*.*:						
cpe:2.3:a:mantisbt:mantisbt:2.0.0:rc1:*.*.*.*.*.*:						
cpe:2.3:a:mantisbt:mantisbt:2.0.0:rc2:*.*.*.*.*.*:						
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:2.1.3:*.*.*.*.*.*:						
cpe:2.3:a:mantisbt:mantisbt:2.2.0:*.*.*.*.*.*:						
cpe:2.3:a:mantisbt:mantisbt:2.2.1:*.*.*.*.*.*:						
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:2.3.0:*.*.*.*.*.*:						
cpe:2.3:a:mantisbt:mantisbt:2.3.1:*.*.*.*.*.*:						
cpe:2.3:a:mantisbt:mantisbt:2.3.2:*.*.*.*.*.*:						
cpe:2.3:a:mantisbt:mantisbt:2.3.3:*.*.*.*.*.*:						
cpe:2.3:a:mantisbt:mantisbt:2.4.0:*.*.*.*.*.*:						
cpe:2.3:a:mantisbt:mantisbt:2.4.1:*.*.*.*.*.*:						
cpe:2.3:a:mantisbt:mantisbt:2.4.2:*.*.*.*.*.*:						
cpe:2.3:a:mantisbt:mantisbt:2.5.0:*.*.*.*.*.*:						
cpe:2.3:a:mantisbt:mantisbt:2.5.1:*.*.*.*.*.*:						

cpe:2.3:a:mantisbt:mantisbt:2.0.0:beta1:*****:
cpe:2.3:a:mantisbt:mantisbt:2.0.0:beta2:*****:
cpe:2.3:a:mantisbt:mantisbt:2.0.0:beta3:*****:
cpe:2.3:a:mantisbt:mantisbt:2.0.0:rc1:*****:
cpe:2.3:a:mantisbt:mantisbt:2.0.0:rc2:*****:
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:2.1.3:*****:
cpe:2.3:a:mantisbt:mantisbt:2.2.0:*****:
cpe:2.3:a:mantisbt:mantisbt:2.2.1:*****:
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:2.3.0:*****:
cpe:2.3:a:mantisbt:mantisbt:2.3.1:*****:
cpe:2.3:a:mantisbt:mantisbt:2.3.2:*****:
cpe:2.3:a:mantisbt:mantisbt:2.3.3:*****:
cpe:2.3:a:mantisbt:mantisbt:2.4.0:*****:
cpe:2.3:a:mantisbt:mantisbt:2.4.1:*****:
cpe:2.3:a:mantisbt:mantisbt:2.4.2:*****:
cpe:2.3:a:mantisbt:mantisbt:2.5.0:*****:
cpe:2.3:a:mantisbt:mantisbt:2.5.1:*****:
cpe:2.3:a:mantisbt:mantisbt:*****:

No vendor comments have been submitted for this CVE

© [CVE.report](#) 2023   |

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](#)