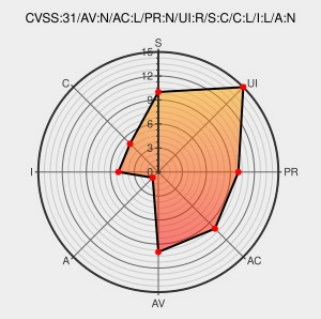
# CVE-2017-12061

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 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 | Third Party Advisory | SECTRACK 1039030 |

| | | |
|---|---|---|
| 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<br>VDB Entry<br>www.securitytracker.com<br>text/html | SECTRACK 1039030 |
| Fix XSS in install.php (CVE-2017-12061) · mantisbt/mantisbt@17f9b94 · GitHub | Patch<br>Third Party Advisory<br>github.com<br>text/html | CONFIRM github.com/mantisbt/mantisbt/commit/17f9b94f031ba93ae2a727bca0e68458ecd08fb |
| oss-security - Re: Advisory: XSS issues in MantisBT (CVE-2017-12061, CVE-2017-12062) | Mailing List<br>Third Party Advisory<br>openwall.com<br>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<br>Third Party Advisory<br>github.com<br>text/html | CONFIRM github.com/mantisbt/mantisbt/commit/c73ae3d3d4dd4681489a9e697e8ade785e27c |
| oss-security - Advisory: XSS issues in MantisBT (CVE-2017-12061, CVE-2017-12062) | Mailing List<br>Third Party Advisory<br>openwall.com<br>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<br>Vendor Advisory<br>mantisbt.org<br>text/html | CONFIRM mantisbt.org/bugs/view.php?id=23146 |



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

← Previous ID

Next ID→

**CVE.report and Source URL Uptime Status status.cve.report**