



CVE-2017-7615

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2017-7615
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-04-16 14:59:00 UTC
Updated	2023-01-20 14:57:00 UTC
Description	MantisBT through 2.3.0 allows arbitrary password reset and unauthenticated admin access via an empty confirm_hash value.

Risk And Classification

Problem Types: CWE-640

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mantisbt	Mantisbt	All	All	All	All

References

Reference	Source	Link
hyp3rlinx.altervista.org/advisories/MANTIS-BUG-TRACKER-PRE-AUTH-REMOTE-PASSWORD-RESET.txt	MISC	hyp3rlinx.altervista.org/advisories/MANTIS-BUG-TRACKER-PRE-AUTH-REMOTE-PASSWORD-RESET.txt
Mantis Bug Tracker 2.3.0 Remote Code Execution ~ Packet Storm	MISC	packetstormsecurity.com/files/42848/Mantis-Bug-Tracker-2.3.0-Remote-Code-Execution.html
0022690: CVE-2017-7615: Account verification page allows resetting any user's password - MantisBT	CONFIRM	mantisbt.org/bug_page.php?id=0022690
oss-security - MantisBT - Full admin access vulnerability	MISC	www.openwall.com/lists/oss-security/2017/04/16/1
MantisBT CVE-2017-7615 Security Bypass Vulnerability	BID	www.securityfocus.com/bid/98444
Mantis Bug Tracker 1.3.0/2.3.0 - Password Reset	EXPLOIT-DB	www.exploit-db.com/exploits/4844/
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

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