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 valu

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.alterv
Mantis Bug Tracker 2.3.0 Remote Code Execution ≈ Packet Storm	MISC	packetstormsec
0022690: CVE-2017-7615: Account verification page allows resetting any user's password - MantisBT	CONFIRM	mantisbt.org
oss-security - MantisBT - Full admin access vulnerability	MISC	www.openwall.(
MantisBT CVE-2017-7615 Security Bypass Vulnerability	BID	www.securityfo
Mantis Bug Tracker 1.3.0/2.3.0 - Password Reset	EXPLOIT-DB	www.exploit-db
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.

Free CVE JSON API cve.report/api

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