CVE-2017-7897

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2017-7897
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-04-18 17:59:00 UTC
Updated	2025-04-20 01:37:25 UTC
Description	A cross-site scripting (XSS) vulnerability in the MantisBT (2.3.x before 2.3.2) Timeline include page, used in My View (my_v

Risk And Classification

Primary CVSS: v3.0 6.1 MEDIUM from nvd@nist.gov

CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

Problem Types: CWE-79 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	6.1	MEDIUM	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
2.0	nvd@nist.gov	Primary	4.3		AV:N/AC:M/Au:N/C:N/I:P/A:N

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

None

CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

AV:N/AC:M/Au:N/C:N/I:P/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mantisbt	Mantisbt	2.3.0	All	All	All
Application	Mantisbt	Mantisbt	2.3.1	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference
Fix XSS in timeline_inc.php · mantisbt/mantisbt@a1c7193 · GitHub
Multiple XSS Fixes by quantumpacket · Pull Request #1094 · mantisbt/mantisbt · GitHub
0022742: CVE-2017-7897: XSS in timeline_inc.php (affects my_view_page.php and view_user_page.php) - MantisBT
MantisBT Input Validation Flaw in 'view_user_page.php' and 'my_view_page.php' Lets Remote Users Conduct Cross-Site Scripting Attacks - S
CVE Program record
NVD vulnerability detail

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**