



CVE-2017-9366

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

Summary

CVE	CVE-2017-9366
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-06-02 05:29:00 UTC
Updated	2020-12-03 16:17:00 UTC
Description	Telaxus EPESI 1.8.2 and earlier has a Stored Cross-site Scripting (XSS) vulnerability in modules/Base/Dashboard/Dashbo

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
github.com/Telaxus/EPESI/commit/36be628c2597fd0209224a09b17858294f49c585	CONFIRM	github.com	Patch, Third Party Advisor
github.com/Telaxus/EPESI/issues/196	CONFIRM	github.com	Exploit, Third Party Advisor
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

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