CVE-2015-2702

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

Summary

CVE	CVE-2015-2702
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-03-25 14:59:07 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Cross-site scripting (XSS) vulnerability in the Message Log in the Email Security Gateway in Websense TRITON AP-EMAIL

Risk And Classification

Primary CVSS: v2.0 4.3 from nvd@nist.gov

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

Problem Types: CWE-79 | n/a

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	Websense	Triton Ap Data	All	All	All	All

Application	Websense	Triton Ap Email	All	All	All	All
Application	Websense	Triton Ap Web	All	All	All	All
Application	Websense	V-series Appliances	7.7	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
Full Disclosure: Websense Email Security vulnerable to persistent Cross-Site Scripting in audit log details view	af854a3a-212
Securify - security advisories - Websense Email Security vulnerable to persistent Cross-Site Scripting in audit log details view	af854a3a-212
Malformed Request	af854a3a-212
SecurityFocus	af854a3a-212
Websense Email Security Cross Site Scripting ≈ Packet Storm	af854a3a-212
Vulnerabilities resolved in TRITON APX Version 8.0	af854a3a-212
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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