CVE-2015-2747

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

Summary

CVE	CVE-2015-2747
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-03-26 14:59:04 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Multiple cross-site scripting (XSS) vulnerabilities in the data loss prevention (DLP) incident Forensics Preview in Websense

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	7.8.3	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
Securify - security advisories - Websense Data Security DLP incident Forensics Preview is vulnerable to Cross-Site Scripting	af854a3a-212
SecurityFocus	af854a3a-212
Websense Data Security DLP Incident Forensics Preview XSS ≈ Packet Storm	af854a3a-212
Full Disclosure: Websense Data Security DLP incident Forensics Preview is vulnerable to Cross-Site Scripting	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.