CVE-2011-1524

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

Summary

CVE	CVE-2011-1524
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-03-28 18:55:00 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Cross-site scripting (XSS) vulnerability in the management login GUI page in Symantec LiveUpdate Administrator (LUA) be

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	Symantec	Liveupdate Administrator	2.1.0	All	All	All

Application	Symantec	Liveupdate Administrator	2.1.2	All	All	All
Application	Symantec	Liveupdate Administrator	2.1.3	All	All	All
Application	Symantec	Liveupdate Administrator	2.2.1	All	All	All
Application	Symantec	Liveupdate Administrator	2.2.2	All	All	All
Application	Symantec	Liveupdate Administrator	All	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
Symantec LiveUpdate Administrator Management GUI HTML Injection Vulnerability	af854a3a-2127-42
sotiriu.de/adv/NSOADV-2011-001.txt	af854a3a-2127-42
Symantec LiveUpdate Administrator CSRF vulnerability - CXSecurity.com	af854a3a-2127-42
Symantec LiveUpdate Administrator Input Validation Flaw Permits Cross-Site Request Forgery Attacks - SecurityTracker	af854a3a-2127-42
SecurityFocus	af854a3a-2127-42
IBM X-Force Exchange	af854a3a-2127-42
Symantec LiveUpdate Administrator Cross-Site Request Forgery	af854a3a-2127-42
Symantec LiveUpdate Administrator Management GUI HTML Injection	af854a3a-2127-42
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-42
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.