CVE-2011-0550

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

Summary

CVE	CVE-2011-0550
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-08-15 19:55:03 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Multiple cross-site scripting (XSS) vulnerabilities in the Web Interface in the Endpoint Protection Manager in Symantec End

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	Endpoint Protection	11.0.6000	All	All	All

Application	Symantec	Endpoint Protection	11.0.6100	All	All	All
Application	Symantec	Endpoint Protection	11.0.6200	All	All	All
Application	Symantec	Endpoint Protection	11.0.6200.754	All	All	All
Application	Symantec	Endpoint Protection	11.0.6300	All	All	All

Vendor Declared Affected Products

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

References

Reference
www.osvdb.org/74465
Symantec Endpoint Protection Manager Cross-Site Scripting and Request Forgery - Secunia.com
Symantec Endpoint Protection Manager Input Validation Hole Permits Cross-Site Scripting and Cross-Site Request Forgery Attacks - Security
Symantec Endpoint Protection CVE-2011-0550 Cross Site Scripting Vulnerability
IBM X-Force Exchange
Security Advisories Relating to Symantec Products - Symantec Endpoint Protection Manager Cross-Site Request Forgery and Cross-Site Scri
www.osvdb.org/74466
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.