CVE-2012-0289

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

Summary

CVE	CVE-2012-0289
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-05-23 21:55:01 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Buffer overflow in Symantec Endpoint Protection (SEP) 11.0.600x through 11.0.710x and Symantec Network Access Contr

Risk And Classification

Primary CVSS: v2.0 7.2 from nvd@nist.gov

AV:L/AC:L/Au:N/C:C/I:C/A:C

Problem Types: CWE-119 | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:L/AC:L/Au:N/C:C/I:C/A:C

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
Application	Symantec	Endpoint Protection	11.0.7000	All	All	All
Application	Symantec	Endpoint Protection	11.0.7100	All	All	All
Application	Symantec	Network Access Control	11.0.6000	All	All	All
Application	Symantec	Network Access Control	11.0.6100	All	All	All
Application	Symantec	Network Access Control	11.0.6200	All	All	All
Application	Symantec	Network Access Control	11.0.6300	All	All	All
Application	Symantec	Network Access Control	11.0.7000	All	All	All
Application	Symantec	Network Access Control	11.0.7100	All	All	All

Vendor Declared Affected Products

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

References

Reference
Symantec Endpoint Protection Bugs Let Remote Users Delete Files and Execute Arbitrary Code and Let Local Users Gain Elevated Privileges
Security Advisories Relating to Symantec Products - Symantec Endpoint Protection Multiple Issues - 2012-05-22T11:31:41 PDT | Symantec
Symantec Endpoint Protection Local Privilege Escalation Vulnerability
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.