CVE-2012-0304

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

Summary

CVE	CVE-2012-0304
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-06-22 10:24:06 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Symantec LiveUpdate Administrator before 2.3.1 uses weak permissions (Everyone: Full Control) for the installation directo

Risk And Classification

Primary CVSS: v2.0 6.9 from nvd@nist.gov

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

Problem Types: CWE-264 | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Medium

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Symantec	Liveupdate Administrator	1.5.3.21	All	All	All

Application	Symantec	Liveupdate Administrator	1.5.4	All	All	All
Application	Symantec	Liveupdate Administrator	1.5.7.19	All	All	All
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	2.2.2.9	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
Nessus Plugin ID 59193 | Tenable Network Security
Security Advisories Relating to Symantec Products - Symantec LiveUpdate Administrator 2.3 Insecure File Permissions - 2012-06-15T10:25:5
Symantec LiveUpdate Administrator Insecure File Permissions Local Privilege Escalation Vulnerability
Symantec LiveUpdate Administrator Lets Local Users Gain Elevated Privileges - SecurityTracker
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.