CVE-2009-0651

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

Summary

CVE	CVE-2009-0651
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-02-20 18:30:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	Unspecified vulnerability in the Veritas network daemon (aka vnetd) in Symantec Veritas NetBackup Server / Enterprise Se

Risk And Classification

Primary CVSS: v2.0 6.5 from nvd@nist.gov

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

Problem Types: CWE-20 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

Single

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Symantec	Veritas Netbackup Server /enterprise Server	5.1	All	All	All

Application	Symantec	Veritas Netbackup Server /enterprise Server	6.0	All	All	All
Application	Symantec	Veritas Netbackup Server /enterprise Server	6.5	All	All	All
Application	Symantec	Veritas Netbackup Server /enterprise Server	All	All	All	All
Application	Symantec	Veritas Netbackup Server /enterprise Server	All	All	All	All
Application	Symantec	Veritas Netbackup Server /enterprise Server	All	All	All	All

Vendor Declared Affected Products

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

References

Reference
Webmail - OVH
Symantec Veritas NetBackup vnetd Lets Remote Authenticated Users Execute Arbitrary Code - SecurityTracker
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
www.securityfocus.com/bid/33772
IBM X-Force Exchange
Symantec Security Advisory
Symantec Veritas NetBackup "vnetd" Server Data Processing Vulnerability - Secunia Advisories - Vulnerability Information - Secunia.com
osvdb.org/52269
Symantec Security Advisory SYM09-002: A non-privileged but authorized system user could potentially leverage the NetBackup network daen
#253287: Security Vulnerability in the VERITAS (Symantec) NetBackup Network Daemon may Allow Escalation of Privileges
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.