



CVE-2008-3703

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2008-3703
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-08-18 17:41:00 UTC
Updated	2018-10-11 20:49:00 UTC
Description	The management console in the Volume Manager Scheduler Service (aka VxSchedService.exe) in Symantec Veritas Storage Foundation for Windows accepts NULL NTLMSSP authentication, which allows remote attackers to bypass authentication and execute arbitrary code via a crafted request.

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Symantec	Veritas Storage Foundation	5.0	All	windows	All
Application	Symantec	Veritas Storage Foundation	5.0	rp1a	windows	All
Application	Symantec	Veritas Storage Foundation	5.1	All	windows	All
Application	Symantec	Veritas Storage Foundation	5.0	All	windows	All
Application	Symantec	Veritas Storage Foundation	5.0	rp1a	windows	All
Application	Symantec	Veritas Storage Foundation	5.1	All	windows	All

References

Reference

Invalid URL

SecurityTracker.com Archives - VERITAS Storage Foundation for Windows Accepts NULL NTLMSSP Authentication

Symantec Veritas Storage Foundation NULL NTLMSSP Authentication Security Bypass - Secunia Advisories - Vulnerability Intelligence - Secunia

404 Not Found

Symantec Storage Foundation for Windows Security Update Circumvention Vulnerability

SecurityFocus

Zero Day Initiative

SYM08-015_SFW_SecurityUpdateBypass - CXSecurity.com

IBM X-Force Exchange
SecurityFocus
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
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.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)