



CVE-2008-4309

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

Summary

CVE	CVE-2008-4309
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-10-31 20:29:00 UTC
Updated	2023-11-07 02:02:00 UTC
Description	Integer overflow in the netsnmp_create_subtree_cache function in agent/snmp_agent.c in net-snmp 5.4 before 5.4.2.1, 5.3

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Net-snmp	Net-snmp	5.2.5	All	All	All
Application	Net-snmp	Net-snmp	5.3.2.2	All	All	All
Application	Net-snmp	Net-snmp	5.4	All	All	All
Application	Net-snmp	Net-snmp	5.2.5	All	All	All
Application	Net-snmp	Net-snmp	5.3.2.2	All	All	All
Application	Net-snmp	Net-snmp	5.4	All	All	All

References

Reference	Source
Net-snmp GETBULK Integer Overflow Denial of Service - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA
Debian -- Security Information -- DSA-1663-1 net-snmp	DEBIAN
SourceForge.net: News: Security releases: 5.4.2.1, 5.3.2.3 and 5.2.5.1	CONFIRM
USN-685-1: Net-SNMP vulnerabilities Ubuntu	UBUNTU
IBM X-Force Exchange	XF
Net-SNMP GETBULK Remote Denial of Service Vulnerability	BID
SUSE update for net-snmp - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA
Sun Solaris SNMP Daemon Denial of Service Vulnerability - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA

Webmail - OVH	VUPEN
About the security content of Time Capsule and AirPort Base Station (802.11n) Firmware 7.5.2	CONFIRM
rPath update for net-snmp - Secunia.com	SECUNIA
Net-SNMP: Denial of Service — Gentoo Linux Documentation	GENTOO
Repository / Oval Repository	OVAL
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
VMware ESX Server update for net-snmp and libxml2 - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA
Security Advisory SA33631 - Gentoo update for net-snmp - Secunia	SECUNIA
469349 – (CVE-2008-4309) CVE-2008-4309 net-snmp: numresponses calculation integer overflow in snmp_agent.c	MISC
Apple Mac OS X Security Update Fixes Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA
Avaya Products Net-snmp GETBULK Denial of Service - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA
About the security content of Security Update 2009-002 / Mac OS X v10.5.7	CONFIRM
US-CERT Technical Cyber Security Alert TA09-133A -- Apple Updates for Multiple Vulnerabilities	CERT
404 Not Found	MISC
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
SecurityFocus	BUGTRAQ
Support / Security / Advisories // MDVSA-2008:225 Mandriva	MANDRIVA
Red Hat Customer Portal	MISC
ASA-2008-467 (RHSA-2008-0971)	CONFIRM
Repository / Oval Repository	OVAL
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
APPLE-SA-2010-12-16-1 Time Capsule and AirPort Base Station (802.11n) Firmware 7.5.2	APPLE
Security Advisory SA32664 - Debian update for net-snmp - Secunia	SECUNIA
262908	SUNALERT
Advisories:rPSA-2008-0315 - rPath Wiki	CONFIRM
Red Hat update for net-snmp - Secunia.com	SECUNIA
oss-security - New net-snmp DoS	MLIST
APPLE-SA-2009-05-12 Security Update 2009-002 / Mac OS X v10.5.7	APPLE
Support	REDHAT
Net-snmp GETBULK Request Processing Bug Lets Remote Users Deny Service - SecurityTracker	SECTRACK
Webmail - OVH	VUPEN
VMSA-2009-0001 - VMware	CONFIRM
Ubuntu update for net-snmp - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA
access.redhat.com CVE-2008-4309	MISC
[security-announce] SUSE Security Summary Report: SUSE-SR:2009:003	SUSE

Repository / Oval Repository	OVAL
'[security bulletin] HPSBMA02447 SSRT090062 rev.1 - Insight Control Suite For Linux (ICE-LX) Cross Si' - MARC	HP
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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](#).

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