



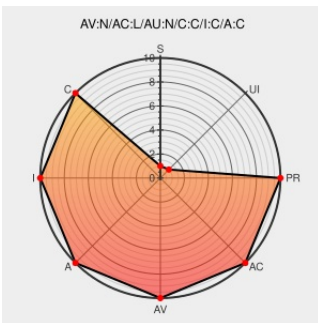
Last Modified on: 03/23/2021 11:27:24 PM UTC

CVE-2005-1740

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF 

Certain versions of [Net-snmp](#) from [Net-snmp](#) contain the following vulnerability:

fixproc in Net-snmp 5.x before 5.2.1-r1 creates temporary files insecurely, which allows local users to modify the contents of those files to execute arbitrary commands, or overwrite arbitrary files via a symlink attack.

CVE-2005-1740 has been assigned by  cve@mitre.org to track the vulnerability

CVSS2 Score: 10 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
rhn.redhat.com Red Hat Support	www.redhat.com text/html	 REDHAT RHSA-2005:373
Secunia - Advisories - Red Hat update for net-snmp	web.archive.org text/html	 SECUNIA 16999
Secunia - Advisories - Mandriva update for net-snmp	web.archive.org text/html	 SECUNIA 18635
SecurityTracker.com Archives - net-snmp 'fixproc' Unsafe Temporary File Lets Local Users Gain Elevated Privileges	securitytracker.com text/html	 SECTrack 1014039
Secunia - Advisories - SGI Advanced Linux Environment Multiple Updates	web.archive.org text/html	 SECUNIA 17135
Net-SNMP Fixproc Insecure Temporary File Creation Vulnerability	cve.report (archive) text/html	 BID 13715

ZATAZ » Page non trouvée	www.zataz.net text/plain Inactive Link Not Archived	 MISC www.zataz.net/adviso/net-snm-05182005.txt
Advisories - Mandriva Linux	www.mandriva.com text/html	 MANDRIVA MDKSA-2006:025
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	 VUPEN ADV-2005-0598
rh.n.redhat.com Red Hat Support	www.redhat.com text/html	 REDHAT RHSA-2005:395
Gentoo Linux Documentation -- Net-SNMP: fixproc insecure temporary file creation	Vendor Advisory security.gentoo.org text/html	 GENTOO GLSA-200505-18
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval.org/mitre.oval:def:11659
No Description Provided	www.osvdb.org Inactive Link Not Archived	 OSVDB 16778
Secunia - Advisories - Net-snm fixproc Insecure Temporary File Creation	web.archive.org text/html	 SECUNIA 15471

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Net-snm	Net-snm	5.0.1	All	All	All
Application	Net-snm	Net-snm	5.0.3	All	All	All
Application	Net-snm	Net-snm	5.0.4_pre2	All	All	All
Application	Net-snm	Net-snm	5.0.5	All	All	All
Application	Net-snm	Net-snm	5.0.6	All	All	All
Application	Net-snm	Net-snm	5.0.7	All	All	All
Application	Net-snm	Net-snm	5.0.8	All	All	All
Application	Net-snm	Net-snm	5.0.9	All	All	All
Application	Net-snm	Net-snm	5.1.2	All	All	All
Application	Net-snm	Net-snm	5.0.1	All	All	All
Application	Net-snm	Net-snm	5.0.3	All	All	All
Application	Net-snm	Net-snm	5.0.4_pre2	All	All	All
Application	Net-snm	Net-snm	5.0.5	All	All	All

Application	Net-snmp	Net-snmp	5.0.6	All	All	All
Application	Net-snmp	Net-snmp	5.0.7	All	All	All
Application	Net-snmp	Net-snmp	5.0.8	All	All	All
Application	Net-snmp	Net-snmp	5.0.9	All	All	All
Application	Net-snmp	Net-snmp	5.1.2	All	All	All
cpe:2.3:a:net-snmp:net-snmp:5.0.1:*:*:*:*:*:						
cpe:2.3:a:net-snmp:net-snmp:5.0.3:*:*:*:*:*:						
cpe:2.3:a:net-snmp:net-snmp:5.0.4_pre2:*:*:*:*:*:						
cpe:2.3:a:net-snmp:net-snmp:5.0.5:*:*:*:*:*:						
cpe:2.3:a:net-snmp:net-snmp:5.0.6:*:*:*:*:*:						
cpe:2.3:a:net-snmp:net-snmp:5.0.7:*:*:*:*:*:						
cpe:2.3:a:net-snmp:net-snmp:5.0.8:*:*:*:*:*:						
cpe:2.3:a:net-snmp:net-snmp:5.0.9:*:*:*:*:*:						
cpe:2.3:a:net-snmp:net-snmp:5.1.2:*:*:*:*:*:						
cpe:2.3:a:net-snmp:net-snmp:5.0.1:*:*:*:*:*:						
cpe:2.3:a:net-snmp:net-snmp:5.0.3:*:*:*:*:*:						
cpe:2.3:a:net-snmp:net-snmp:5.0.4_pre2:*:*:*:*:*:						
cpe:2.3:a:net-snmp:net-snmp:5.0.5:*:*:*:*:*:						
cpe:2.3:a:net-snmp:net-snmp:5.0.6:*:*:*:*:*:						
cpe:2.3:a:net-snmp:net-snmp:5.0.7:*:*:*:*:*:						
cpe:2.3:a:net-snmp:net-snmp:5.0.8:*:*:*:*:*:						
cpe:2.3:a:net-snmp:net-snmp:5.0.9:*:*:*:*:*:						
cpe:2.3:a:net-snmp:net-snmp:5.1.2:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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](#)