



CVE-2005-4552

Published on: 12/28/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:22 PM UTC

CVE-2005-4552

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Solaris Pc Netlink](#) from [Sun](#) contain the following vulnerability:

The (1) slsmgr and (2) slsadmin programs in Sun Solaris PC NetLink 2.0 create temporary files insecurely, which allows local users to gain privileges.

CVE-2005-4552 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.2 - HIGH**

Access
Vector

LOCAL

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

SecurityTracker.com Archives - PC NetLink 'slsmgr' Unsafe Temporary Files Lets Local Users Gain Elevated Privileges

Patch
[securitytracker.com](#)
text/html

[SECTrack 1015408](#)

No Description Provided

Patch
Vendor Advisory
[sunsolve.sun.com](#)

[SUNALERT 102122](#)

Inactive Link Not Archived

Repository / Oval Repository

[oval.cisecurity.org](#)
text/html

[OVAL](#)
oval.org.mitre.oval:def:1409

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#)
text/html

[XF sun-pcnetlink-slsadmin-insecure\(23853\)](#)

Sun Solaris PC NetLink Insecure Permissions Vulnerability

[cve.report \(archive\)](#)

[BID 16059](#)

[text/html](#)

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

[www.vupen.com](#) VUPEN ADV-2005-3083[text/html](#)

No Description Provided

[Patch](#) SUNALERT 102117[Vendor Advisory](#)[sunsolve.sun.com](#)[Inactive Link](#)[Not Archived](#)

Sun Solaris PC NetLink Insecure File Handling Vulnerability - Secunia Advisories - Vulnerability Intelligence - Secunia.com

[Patch](#) SECUNIA 18230[Vendor Advisory](#)[web.archive.org](#)[text/html](#)

SecurityTracker.com Archives - PC NetLink 'slsadmin' Unsafe Temporary Files Lets Local Users Gain Elevated Privileges

[Patch](#) SECTrack 1015409[securitytracker.com](#)[text/html](#)

No Description Provided

[www.osvdb.org](#) OSVDB 22045[Inactive Link](#)[Not Archived](#)

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#) XF sun-pcnetlink-slsmgr-insecure(23851)[text/html](#)

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	Sun	Solaris Pc Netlink	2.0	All	All	All
Application	Sun	Solaris Pc Netlink	2.0	All	All	All

cpe:2.3:a:sun:solaris_pc_netlink:2.0:*:*:*:*:*:

cpe:2.3:a:sun:solaris_pc_netlink:2.0:*:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)[Next ID →](#)© CVE.report 2023   |

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