

[UNIX] Solaris PC Netlink Insecure File Handling

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-12/msg00107.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 28 Dec 2005 11:57:50 +0200
-

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Solaris PC Netlink Insecure File Handling

SUMMARY

" <<http://www.sun.com/solaris/>> Solaris PC <<http://www.sun.com/products/interoperability/netlink/>> NetLink software (based on AT&T Advanced Server for Unix) delivers native Windows NT network services--which include directory, authentication, and file-and-print services--on Solaris environment servers."

A vulnerability within PC Netlink allows locally stored files to be opened insecurely and possibly modified.

DETAILS

Vulnerable Systems:

- * PC NetLink 2.0 (for Solaris 7, 8 and 9) without patch 121209-01

Immune Systems:

- * PC NetLink 2.0 (for Solaris 7, 8 and 9) with patch 121209-01 or later

A security vulnerability in the "/opt/lanman/sbin/slsmgr" and "/etc/init.d/slsadmin" command in PC NetLink allows files to be opened insecurely, which could allow an unprivileged local user the ability to

[UNIX] Solaris PC Netlink Insecure File Handling

write to the filesystem with the permissions of the user running the script. If the script is run as "root," it may allow a local unprivileged user to gain elevated privileges on the system and run arbitrary commands.

ADDITIONAL INFORMATION

The original article can be found at:

<<http://sunsolve.sun.com/searchproxy/document.do?assetkey=1-26-102117-1>>
<http://sunsolve.sun.com/searchproxy/document.do?assetkey=1-26-102117-1>
<<http://sunsolve.sun.com/searchproxy/document.do?assetkey=1-26-102122-1>>
<http://sunsolve.sun.com/searchproxy/document.do?assetkey=1-26-102122-1>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

-
- Prev by Date: [*\[NEWS\] BZFlag Server DoS*](#)
 - Next by Date: [*\[NT\] RunAs Allows Bypassing User GPO in Windows XP/2003*](#)
 - Previous by thread: [*\[NEWS\] BZFlag Server DoS*](#)
 - Next by thread: [*\[NT\] RunAs Allows Bypassing User GPO in Windows XP/2003*](#)
 - Index(es):
 - ◆ [*Date*](#)
 - ◆ [*Thread*](#)