

[UNIX] HP-UX Setuid RLPDaemon Illicit File Writes

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-12/0090.html>

From: support@securiteam.com

Date: 12/21/01

From: support@securiteam.com

To: list@securiteam.com

Date: Fri, 21 Dec 2001 13:03:33 +0100 (CET)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

HP-UX Setuid RLPDaemon Illicit File Writes

SUMMARY

/usr/sbin/rlpdaemon in HP-UX is setuid root. Its switches include "-l" to enable logging and "-L /some/thing" to select a logfile other than the default. When run by a non-root user it can create/append a logfile owned by root. With a little care (and a copy of RFC1179), a local user can supply data to add to files he chooses and thereby get root. The victim does not actually need to have any printers configured.

DETAILS

Vulnerable systems:

HP-UX 10.20

HP-UX 11.00

Example:

As a non-root user run:

```
$ rlpdaemon -i -l -L /existing_directory/new_file
```

If the logfile created is owned by root you have the bug. Patched systems

quit silently if "-i" is used and print "Unable to open/create logfile"

if "-l -L" is used.

Solution:

HP's alert "Sec. Vulnerability in rlpdaemon" (HPSBUX0111-176) was released

Securiteam: [UNIX] HP-UX Setuid RLPDaemon Illicit File Writes

2001-11-20 and describes this as a "logic flaw vulnerability". Because the patches fix more than one problem you should definitely aim to have them installed unless you remove rlpdaemon.

ADDITIONAL INFORMATION

The information has been provided by <mailto:borglum@nym.alias.net>
G.Borglum.

=====

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@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

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.

-
- **Previous message:** support@securiteam.com: "[NEWS] Novell GroupWise Servlet Gateway Default Username and Password"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)