

[UNIX] Logic Flaw in HP-UX Line Printer Daemon Leads to Remote Code Execution

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-11/0052.html>

From: support@securiteam.com

Date: 11/25/01

From: support@securiteam.com

To: list@securiteam.com

Subject: [UNIX] Logic Flaw in HP-UX Line Printer Daemon Leads to Remote Code Execution

Message-Id: <20011125224703.C8C3D138BF@mail.der-keiler.de>

Date: Sun, 25 Nov 2001 23:47:03 +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.

Logic Flaw in HP-UX Line Printer Daemon Leads to Remote Code Execution

SUMMARY

Internet Security Systems (ISS) X-Force has discovered a vulnerability in the HP-UX line printer daemon (rpldaemon). This vulnerability may allow a remote or local attacker to execute arbitrary code with superuser privilege.

DETAILS

Vulnerable systems:

HP-UX version 10.01

HP-UX version 10.10

HP-UX version 10.20

HP-UX version 11.00

HP-UX version 11.11

The line printer daemon allows printer sharing over a network of UNIX computers. HP-UX is shipped with a line printer daemon adapted from BSD Unix. The HP line printer daemon is similar to "in.lpd" in other UNIX variants.

Securiteam: [UNIX] Logic Flaw in HP-UX Line Printer Daemon Lead

A vulnerability exists in rlpdaemon that may allow remote attackers to send specially-crafted print requests, which can be used to create arbitrary files or directories on the target system. Given the ability to write to arbitrary files, remote attackers may gain access to the target system.

The rlpdaemon daemon is enabled by default and executed with superuser privilege. This vulnerability can be successfully exploited with no local account or specific knowledge of the target system's configuration.

Recommendations:

ISS X-Force recommends that all system administrators who have not implemented network printing should immediately disable rlpdaemon and any other unused services. HP will make the following patches available to address the vulnerability described in this advisory:

HP-UX 10.01 PHCO_25107
HP-UX 10.10 PHCO_25108
HP-UX 10.20 PHCO_25109
HP-UX 11.00 PHCO_25110
HP-UX 11.11 PHCO_25111

To access these patches when they become available, visit:

<<http://itrc.hp.com>> <http://itrc.hp.com>

ADDITIONAL INFORMATION

The information has been provided by <<mailto:xforce@iss.net>> X-Force.

=====

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: "[TOOL] Snort-rep, Snort Text/HTML Reporting Tool"
 - *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)