

[UNIX] HPUX 'Disable' Buffer Overflow Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-02/0030.html>

From: support@securiteam.com

Date: 02/15/03

From: support@securiteam.com

To: list@securiteam.com

Date: 15 Feb 2003 21:31:27 +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

Beyond Security would like to welcome Tiscali World Online to our service provider team.

For more info on their service offering IP-Secure, please visit http://www.worldonline.co.za/services/work_ip.asp

HPUX 'Disable' Buffer Overflow Vulnerability

SUMMARY

The 'dis/enable' command activates the named printers, enabling them to print requests taken by lp. The "-r" option associate a reason with the deactivation of the printer. The "-c" option cancel any requests that are currently printing on any of the designated printers. By executing a 'disable' command with a long reason the lp daemon can be caused to overflow one of its internal buffers, allowing the execution of arbitrary code.

DETAILS

Vulnerable systems:

* HP9000 Servers running HP-UX releases 10.20, 11.00, and 11.11 (11i).

Example:

```
$ ls -al `which disable`  
-r-sr-xr-x 1 lp bin 28672 Jun 15 1998  
/usr/bin/disable
```

Using disable with or without '-r', '-c' with a long option string:

Securiteam: [UNIX] HPUX 'Disable' Buffer Overflow Vulnerability

```
$ disable -r `perl -e 'printf "A" x 9777`  
Memory fault
```

Vendor response:

We have contacted Davide Del Vecchio and confirmed that the the buffer overflow in disable(1) does not occur with the patches recommended in HPSBUX0208-213.

ADDITIONAL INFORMATION

The information has been provided by <mailto:dante@alighieri.org> Davide Del Vecchio.

=====

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.