

Re: Sec. Vulnerability in OpenSSH on HP-UX

Source: <http://www.derkeiler.com/Newsgroups/comp.security.misc/2002-06/0437.html>

From: sjk (sjk@panda.dredel.com)

Date: 06/27/02

From: sjk <sjk@panda.dredel.com>
Date: Thu, 27 Jun 2002 21:37:54 -0000

I guess this doesn't effect 10.20 -- as there is no Pam??

In article <[affqk8\\$ria\\$2@web1.cup.hp.com](mailto:affqk8ria2@web1.cup.hp.com)>, Security Alert wrote:

> -----BEGIN PGP SIGNED MESSAGE-----

> Hash: SHA1

>
>

> HEWLETT-PACKARD COMPANY SECURITY BULLETIN: #0195,

> Originally issued: 27 June 2002

>

>

> The information in the following Security Advisory should be acted
> upon as soon as possible. Hewlett-Packard Company will not be
> liable for any consequences to any customer resulting from customer's
> failure to fully implement instructions in this Security Advisory as
> soon as possible.

>
>

> **PROBLEM:** OpenSSH input validation errors can cause faults from
> remote hosts in SSH protocol version 2.

>

> **PLATFORM:** HP 9000 Servers running HP-UX release 11.00, and 11.11
> only with the T1471AA SSH product installed.

>

> **DAMAGE:** Possible privilege increases, from remote locations.

>

> **SOLUTION:** Disable PAMAuthenticationViaKbdInt in sshd_config.

>

> **MANUAL ACTIONS:** Edit sshd_config appropriately.

>

> **AVAILABILITY:** n/a

>
>

comp.security.misc: Re: Sec. Vulnerability in OpenSSH on HP-UX

- > *A. Background*
- > Pursuant to the CERT Advisory CA-2002-18 on OpenSSH,
- > Hewlett-Packard Company has learned of a defect in the
- > code in SSH, product number T1471AA.
- >
- >
- > *B. Fixing the problem*
- > As a short-term solution, disable `PAMAuthenticationViaKbdInt`
- > in the `sshd_config` file; i.e.,
- >
- > `PAMAuthenticationViaKbdInt no`
- >
- > The CERT advisory mentions adding the following line to
- > `/etc/ssh/sshd_config`:
- > `ChallengeResponseAuthentication no`
- > NOTE:
- > `ChallengeResponseAuthentication` is not used in the HP product.
- >
- > HP is working to produce a patch for its version which is based
- > on OpenSSH release 3.1p1. This advisory will be updated to a
- > bulletin when that patch is released.
- >
- >
- > *C. To subscribe to automatically receive future NEW HP Security*
- > *Bulletins from the HP IT Resource Center via electronic*
- > *mail, do the following:*
- >
- > Use your browser to get to the HP IT Resource Center page at:
- >
- > <http://itrc.hp.com>
- >
- > Use the 'Login' tab at the left side of the screen to login
- > using your ID and password. Use your existing login or the
- > "Register" button at the left to create a login, in order to
- > gain access to many areas of the ITRC. Remember to save the
- > User ID assigned to you, and your password.
- >
- > In the left most frame select "Maintenance and Support".
- >
- > Under the "Notifications" section (near the bottom of
- > the page), select "Support Information Digests".
- >
- > To -subscribe- to future HP Security Bulletins or other
- > Technical Digests, click the check box (in the left column)
- > for the appropriate digest and then click the "Update
- > Subscriptions" button at the bottom of the page.
- >
- > or
- >
- > To -review- bulletins already released, select the link
- > (in the middle column) for the appropriate digest.

>
> *To –gain access– to the Security Patch Matrix, select*
> *the link for "The Security Bulletins Archive". (near the*
> *bottom of the page) Once in the archive the third link is*
> *to the current Security Patch Matrix. Updated daily, this*
> *matrix categorizes security patches by platform/OS release,*
> *and by bulletin topic. Security Patch Check completely*
> *automates the process of reviewing the patch matrix for*
> *11.XX systems.*
>
> *For information on the Security Patch Check tool, see:*
> *[http://www.software.hp.com/cgi-bin/swdepot_parser.cgi/cgi/](http://www.software.hp.com/cgi-bin/swdepot_parser.cgi/cgi/displayProductInfo.pl?productNumber=B6834AA)*
> *displayProductInfo.pl?productNumber=B6834AA"*
>
> *The security patch matrix is also available via anonymous*
> *ftp:*
>
> *ftp.itrc.hp.com:~ftp/export/patches/hp-ux_patch_matrix*
>
> *On the "Support Information Digest Main" page:*
> *click on the "HP Security Bulletin Archive".*
>
>
> *D. To report new security vulnerabilities, send email to*
>
> *security-alert@hp.com*
>
> *Please encrypt any exploit information using the*
> *security-alert PGP key, available from your local key*
> *server, or by sending a message with a –subject– (not body)*
> *of 'get key' (no quotes) to security-alert@hp.com.*
>
> *Permission is granted for copying and circulating this*
> *Advisory to Hewlett-Packard (HP) customers (or the Internet*
> *community) for the purpose of alerting them to problems,*
> *if and only if, the Advisory is not edited or changed in*
> *any way, is attributed to HP, and provided such reproduction*
> *and/or distribution is performed for non-commercial purposes.*
>
> *Any other use of this information is prohibited. HP is not*
> *liable for any misuse of this information by any third party.*
>
> _____
>
> -----BEGIN PGP SIGNATURE-----
> Version: PGP Personal Security 7.0.3
>
> *iQA/AwUBPRtqeeAfOvwKtKn1ZEQKuSQcG4tbbfPnQ0EOVuUYn1KF9KSMlzMkAnRyW*
> *p1QleW00/wl1NrAQboXwS2T+*
> *=NPuo*
> -----END PGP SIGNATURE-----
>

comp.security.misc: Re: Sec. Vulnerability in OpenSSH on HP-UX

>
> --
> *Yours truly,*
> *HP S/W Security Team*
> *WTEC Cupertino, California*
>
> *Return-Path: secure@cup.hp.com*
> *Reply-to: security-alert@hp.com*

--
----- Aude Sepere -----
sjk@dredel.com
<http://www.dredel.com>
----- Audax et Cautus -----

- ***Next message:*** Walter Roberson: "Re: Computer monitoring programs"
- ***Previous message:*** Wes Gamble: "Connection hijacking in SQL Server 2000"
- ***In reply to:*** Security Alert: "Sec. Vulnerability in OpenSSH on HP-UX"
- ***Messages sorted by:*** [date] [thread] [subject] [author] [attachment]