



Products

Services

Publications

Resources

What's new

Follow @Openwall on Twitter for new release announcements and other news

[<prev] [next>] [<thread-prev] [thread-next>] [day] [month] [year] [list]

Message-Id: <20150723042717.C1C05B2E4B6@smtpvbsrv1.mitre.org>

Date: Thu, 23 Jul 2015 00:27:17 -0400 (EDT)

From: cve-assign@...re.org

To: isowarez.isowarez.isowarez@...glemail.com

Cc: cve-assign@...re.org, oss-security@...ts.openwall.com

Subject: Re: CVE Request for OpenSSH vulnerability - authentication limits bypass

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

Hash: SHA1

As far as we can tell, the essence of the vulnerability is that the client shouldn't be able to specify an arbitrarily large number of KbdInteractiveDevices and be entitled to have the server cooperate. Use CVE-2015-5600.

Here are additional notes in case anyone was expecting two CVE IDs.

The patch at:

<http://cvsweb.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/auth2-chall.c>

<http://cvsweb.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/auth2-chall.c.diff?r1=1.42&r2=1.43&f=h>

seems to suggest a very similar decision. With this change, the server no longer cooperates even with:

```
-oKbdInteractiveDevices=pam,pam
```

and this makes sense because, if a client is behaving normally, using pam a second time would typically just waste server resources, and would not increase usability from the client's perspective. The only exception we've thought of is a server that sometimes makes false-negative access-control decisions, e.g., either it is intentionally designed to be inconsistent, or uses an intermittently available hardware authentication device. In the latter case, maybe users were actually supposed to do something like:

```
-oKbdInteractiveDevices=iahad,iahad,iahad
```

and the patch would have to be revised to support that.

More importantly, we don't think the issue should be characterized as a "MaxAuthTries bypass." If there are several different keyboard-interactive methods supported by the server, and there's a use case in which the client user can type in a single string and have the client program attempt all of the keyboard-interactive methods, then the server arguably shouldn't block any if MaxAuthTries is reached. From the perspective of the client user, it's only one try.

Example: MaxAuthTries has its default value of six, but MIT-KIT has suddenly released six new major Kerberos protocol versions, and the legitimate user enters:

```
-oKbdInteractiveDevices=krb5,krb6,krb7,krb8,krb9,krb10,krb11
```

We don't think it's necessarily correct to block use of the krb11 protocol because it's the seventh one.

This might not be a completely valid example. The essential point is that we don't feel there's a remaining vulnerability in which a MaxAuthTries value of N is supposed to prevent a command line with N+1 different supported elements in the KbdInteractiveDevices list. There is no CVE ID tied directly to the concept of a MaxAuthTries bypass.

- - -

CVE assignment team, MITRE CVE Numbering Authority

M/S M300

202 Burlington Road, Bedford, MA 01730 USA

[PGP key available through http://cve.mitre.org/cve/request_id.html]

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.4.14 (SunOS)

```
iQEcBAEBAGBQJVsGvBAAoJEKl1VAevmvsIl8H/ieb0+Sk56RvkQWMX7PPH68p
GsizwMKpTCiGpmqHLSLoILLj3Pg457BaVnf4inLJQjFezIjtXpnSotIa85PiEfad
t2o6Igx6Kulb9aWeEjxhd3cNCTtrNsg4t6V+Ex6BtPPwTmaibyzXngW/1C5mfRzC
n5C5VZA8lo0yswQ19Dm1oRA/nb5FRha6lBeDDfIMwLATY8v1aChNt0staHePYoLf
8gNdRAvJGmP6EsZJ8Kycgn/hAwnyetL83ZAXa4oa00/CKDr0sP0ip2uIRW9IySqF
5/sffgeb9Ea5Scwke8KBDHZzERgfBYHNza21N6aAoDhzcZHovPHuptZu0R7XxWk=
=oFQW
```

-----END PGP SIGNATURE-----

[Powered by blists](#) - [more mailing lists](#)

Please check out the [Open Source Software Security Wiki](#), which is counterpart to this [mailing list](#).

Confused about [mailing lists](#) and their use? [Read about mailing lists on Wikipedia](#) and check out these [guidelines on proper formatting of your messages](#).