Bug 2387 - sshd treats certificate extensions as critical

Status: CLOSED FIXED

Alias: None

Product: Portable OpenSSH
Component: sshd (show other bugs)
Version: 6.8p1
Hardware: amd64 Linux

Importance: P5 normal
Assignee: Damien Miller

URL:
Keywords:

Depends on:
Blocks: ~~V_6_9~~
Show dependency tree / graph

Reported: 2015-04-22 01:28 EST by Bob Van Zant
Modified: 2015-08-11 23:02 EST (History)
CC List: 2 users (show)

See Also:

Attachments		
accept unrecognised extensions (472 bytes, patch) 2015-04-22 09:50 EST, Damien Miller	dtucker: ok+	Details | Diff
Add an attachment (proposed patch, testcase, etc.)		View All

Note
You need to log in before you can comment on or make changes to this bug.

Bob Van Zant 2015-04-22 01:28:43 EST Description

sshd is treating certificate extensions as critical and is disallowing logins using certificates with unknown extensions. This is happening with v01 certificates and actually the bug is quite obvious when looking for it in the code.

While I am abusing this feature somewhat to encode additional data in a certificate such that it is covered by the certificate's signature this bug has the more serious side effect that it will break backwards compatibility in the future. If OpenSSH adds new cert extensions in a new version older versions of sshd (all versions prior to 6.8) will reject those certificates even though the extensions are supposed to be optional.

Here's a sample certificate's ssh-keygen output:

```
        Type: ssh-rsa-cert-v01@openssh.com user certificate
        Public key: RSA-CERT 1c:fd:36:27:db:48:3f:ad:e2:fe:55:45:67:b1:47:99
        Signing CA: RSA 62:af:90:1b:ef:b1:5a:c9:e0:2a:be:8b:3e:a9:25:18
        Key ID: "bvanzant+stage@brkt.com"
        Serial: 1
        Valid: from 2015-04-21T07:09:30 to 2015-04-21T09:11:30
        Principals:
                ec2-user
                ubuntu
        Critical Options: (none)
        Extensions:
                ca-environment UNKNOWN OPTION (len 5)
                ca-reason UNKNOWN OPTION (len 17)
                permit-agent-forwarding
                permit-port-forwarding
                permit-pty
```

Notice the two non-standard extensions. When I attempt to use this certificate sshd logs:

```
sshd[30925]: error: Certificate critical option "ca-environment" is not supported
```

The relevant code is at lines 597 and 603 of auth-options.c
http://cvsweb.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/auth-options.c?annotate=1.65

Notice the fourth parameter is set to 1 in both the critical and extensions cases. This tells parse_option_list to treat the things being parsed as critical. I believe that the call on line 603 should have crit set to 0.

Darren Tucker 2015-04-22 09:36:07 EST Comment 1

Leaving aside the discussion of this particular bug, if you are adding your own extensions to the certificates you should probably be using your own namespace (ie $foo@$yourdomain, as per RFC4251 section 6), otherwise you risk future breakage if OpenSSH adds a like-named one.

Damien Miller 2015-04-22 09:50:57 EST Comment 2

Created attachment 2598 [details]
accept unrecognised extensions

Yeah, that's wrong. (Do follow Darren's advice though)

Damien Miller 2015-04-22 11:24:16 EST Comment 3

committed - this will be in openssh-6.9

Bob Van Zant 2015-04-23 00:12:14 EST Comment 4

You guys are fast, thank you. And I'll change the format of my extension names, thank you for pointing that out.

Damien Miller 2015-08-11 23:02:27 EST Comment 5

Set all RESOLVED bugs to CLOSED with release of OpenSSH 7.1

Format For Printing - XML - Clone This Bug - Top of page