parabola-hackers - Bug #1068

[parabola-hackers-nshd] Local DoS attack by using long strings.

2016-08-02 04:09 PM - lukeshu

Status:	fixed	**% Done:**	100%
Priority:	bug		
Assignee:	lukeshu		
Category:			

Description

One can make /usr/lib/parabola-hackers/nshd consume huge amounts of memory and crash by sending it a request (at the socket /var/run/nslcd/socket) with a very long string. Note that the nslcd protocol represents a string as a 32-bit length, then a sequence of bytes. This allows the attacker to simply put a large number as the string length, and not actually send that much data. This will cause nshd to allocate memory to store the string. Once the request is handled (or aborted), the garbage collector will "free" the memory, but this only marks it as safe to re-use within nshd; it isn't handed back to the operating system. If the attack is repeated, this will usually resolve itself by causing nshd to OOM-crash and restart.

I do not believe it is possible to use this with remote attacks (for example, by getting sshd to look up a 3GB-long username) because NSS will protect us from funny requests.

Possible fixes:

- Use systemd to specify a maximum memory usage; causing the allocation to fail. This would cause nshd to crash and restart. This could potentially be used by a local attacker to cause nshd to restart while /var/lib/hackers-git/ is in an invalid state (such as if they time it to crash exactly as git pull is running).
- Have a separate process per-request. This would be easy to implement, but we would need to do flock(2)@ing around access to /var/lib/hackers-git@ to avoid situations similar to the above attack. There are also latency concerns with this; but avoiding having another daemon running as root does avoid some security concerns.
- Code in a sane upper-bound for string lengths, and abort requests that use longer strings. Should be easy, but I don't know what a sane upper-bound should be.

Severity: Low; we generally trust local users.

History

#1 - 2017-01-21 12:13 AM - lukeshu

- Project changed from libretools to parabola-hackers

#2 - 2017-04-19 11:46 PM - lukeshu

- Description updated

I really don't want to personally write the code, but: I no longer believe that nshd should be a daemon. I believe that it should be implemented as an nss module and as a pam module.

As much as I love Go, I don't believe that we should have to load the Go runtime into essentially every process; so writing the modules in Go is out. Maybe rust, but probably C.

OTOH, perhaps a standard SQL nss/pam module would be the way to go, and have it load the data into SQL.

I'm liking the idea of using SQL as an ACID cache for things for which the authoritative source is in git.

#3 - 2017-09-09 07:07 PM - lukeshu

- % Done changed from 0 to 100

- Assignee set to lukeshu

- Status changed from open to fixed

fixed in v20170908