Shellshock – The SIP Proxy Edition

Nir Zigler, 2014-01-10

The recent Shellshock and Heartbleed vulnerabilities have something in common – they both affect very infrastructural services.
That is the reason their magnitude is much bigger than any other ol' vulnerability out there.
"Everyone" uses bash, "everyone" uses OpenSSL.

Shock the shell

However, one of the differences is that bash isn't a public facing service like OpenSSL.
Bash is simply the shell service of the underlying operating system.
To be able to get to bash and exploit the vulnerability – one has to find a way to remotely "talk" with and feed it their evil commands via environment variables.

Arguably, the most common path to reach bash is through a web server that makes use of the CGI technology.
By default, CGI creates user-controlled environment variables, which are then parsed by bash, for every HTTP request the server accepts.
This means that exploiting bash on such a system is as easy as sending an HTTP request to a CGI controlled page.

However, CGI isn't the only service that uses bash "behind the scenes".
DHCP services are affected, SSH and Telnet are affected, FTP services are affected.

Some SIP proxies are also affected, we will learn why and how to mitigate them.

SIP Express Router and friends

Popular open source SIP proxies, such as Kamailio, have been found vulnerable to Shellshock.
The author of a POC tool called sipshock has written a very clear explanation on the matter:

The exec module in Kamailio, Opensips and probably every other SER fork passes the received SIP headers as environment variables to the invoking shell. This makes these SIP proxies vulnerable to CVE-2014-6271 (Bash Shellshock). If a proxy is using any of the exec functions and has the 'setvars' parameter set to the default value '1' then by sending SIP messages containing a specially crafted header we can run arbitrary code on the proxy machine.

This means that if you have a public facing SIP proxy running a SIP Express Router implementation, you should patch your bash immediately.

If you have an F5 LTM doing load balancing for that SIP server – a simple iRule will save you the headache of patching the operating system, and give you breathing room to do so properly.

Mitigate Shellshock SIP with BIG-IP iRules

The following iRule will detect SIP requests which contain the Shellshock pattern in one of the headers:

```
when CLIENT_DATA {
                set sCVEPattern "*: () \{*"
                set bCVEFound 0
                if { [string match $sCVEPattern [UDP::payload]] } {
                     set bCVEFound 1
                }
}
when SIP_REQUEST {
                if { $bCVEFound } {
                     log local0. "Detected CVE-2014-6271 Shellshock attack! IP: '[IP::client_addr]'
```

```
From: [SIP::from] To: [SIP::to]"
                    reject
                }
}
```

Create a new iRule and attach it to your SIP proxy virtual server.
Make sure the Virtual Server has “UDP” set as protocol, and is assigned with a SIP profile.

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com