CVE-2014-6271 Shellshocked

Jeff Costlow, 2014-24-09

It's a good thing we are naming all of our vulnerabilities now; it's easier to keep track of them. I haven't seen an official designation for CVE-2014-6271, but Shellshock seems appropriate.

This new vulnerability may allow a remote attacker to execute instructions on your computer using a feature of the bash shell. A shell is a command line user interface with complicated features akin to programming languages. One feature of bash is to take user input from its environment. Unfortunately this environment can contain executable commands and in some cases can be manipulated by a remote user.

F5 has confirmed that BIG-IP's web GUI is vulnerable to an authenticated user. We currently know of no unauthenticated exploits, either against the management interface or against the traffic interfaces.

We can enumerate through RedHat's security blog's list -- not a comprehensive list -- to look at some ways a BIG-IP could be exploited.

- BIG-IP does not use ForceCommand in sshd_config, so users cannot bypass ForceCommand.
- BIG-IP does not contain any bash CGI programs, although it is possible that some CGI programs spawn subshells.
- BIG-IP does contain mod_php, but the scripts are not vulnerable.
- BIG-IP does contain DHCP dhclient and is in theory vulnerable to a malicious DHCP server. This is the only known unauthenticated remotely exploitable vector at this time and is only vulnerable on the management interface. You may disable DHCP on the System::Platform page.
- BIG-IP limits the use of bash to authenticated Administrator level accounts. Non-Administrators only have access to tmsh and do not have access to bash.

We still do not believe the traffic passing interfaces of a BIG-IP can be exploited. Please protect your management interface and ensure that it is not exposed to the internet.

F5 will be patching CVE-2014-6271 on all BIG-IP releases. Sol15629 has been published.

Update: BIG-IP iRule mitigation has been posted. F5 LineRate has posted their mitigation. ASM has signature updates.

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