REN-ISAC

Advisory

September 25, 2014

To: IT Executives and Security Staff

CRITICAL vulnerability In Bash (shellshock)

The REN-ISAC [1] wants to raise awareness and stimulate immediate action concerning a CRITICAL software vulnerability with HIGH LIKLIHOOD OF IMPACT to your institution, and make ourselves available for questions and assistance in understanding the issue. IMMEDIATE ACTION is advised. Active reconnaissance for vulnerable systems and exploitation have been observed. The vulnerability is very easy to exploit; tools and how-to information are easily obtained.

What Are The Vulnerable Services?

GNU Bash through 4.3 bash 43-025

The vulnerability may be exposed through:

- Web services, particularly CGI-based, that invoke bash underneath. It may be difficult to identify servers that expose the vulnerability. It's best to assume that you're vulnerable and exposed. Patch or mitigate accordingly. This path for the vulnerability allows unauthenticated remote exploitation.
- Interfaces in network appliances (routers, firewalls, &c) and embedded control systems. Possibly via unauthenticated remote exploitation and possibly involving shell invocations at privileged levels.
- DHCP, Linux printing (CUPS) and potentially other services that call system() without sanitizing input.

IMMEDIATE ACTION

- Review the Resources identified below.
- Identify vulnerable systems, evaluate your risk profile, and patch systems or otherwise mitigate the risk with due urgency.
- Communicate regarding this risk to your local IT community - make sure that servers managed by various departments and schools are mitigated.

CONTINUING ACTION

- The original patch may not mitigate the problem completely, system maintainers should go ahead and patch anyway and prepare for a second round of patching as more complete fixes become available.
- Monitor for additional information concerning the vulnerability and patches.

- Monitor your network for attack traffic and mitigate those attacks, too

What's At Risk?

It varies upon how specific applications or services invoke bash underneath, but could range from simple information disclosure to complete control over the affected system. It's important to note that risk to your enterprise not only involves internal services but includes use of services provided by other parties, e.g. financial, cloud, &c.

Background

Bash (the "Bourne again shell") is a widely distributed and utilized Unix shell. It's the default shell on Linux and Mac OS X and has been ported to other operating systems (Windows, DOS, Netware, Android) and is used in Unix emulators underneath Windows (e.g. Cygwin). Although many persons associate terminal sessions with bash it is often employed in the background by other applications, for example by web applications making system calls to execute various functions. The name "shellshock" is widely used to name the vulnerability.

The vulnerability allows arbitrary code to be executed on an attacked system by setting environment variables and invoking bash. Systems running web CGI programs that invoke system calls are at very high risk because of the way CGI requires the web server to convert HTTP request headers to environment variables. Other web-based software platforms are also at risk.

Is My Enterprise Affected?

Most likely, yes. Either directly (services that you operate and provide) or indirectly (services provided to you by other parties).

What Systems Are Vulnerable? Are Patches available?

System vulnerability and patch information is quickly evolving. Track at the NIST, US-CERT, and SANS web pages:

CVE-2014-6271 (original vulnerability):

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6271

CVE-2014-7169 (new vulnerability identified due to an incomplete fix for CVE-2014-6271):

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-7169

US-CERT - Bourne Again Shell (Bash) Remote Code Execution Vulnerability:

https://www.us-cert.gov/ncas/current-activity/2014/09/24/Bourne-Again-Shell-Bash-Remote-Code-Execution-Vulnerability

Additional Valuable Resources

SANS - Update on CVE-2014-6271: Vulnerability in bash (shellshock):

https://isc.sans.edu/diary/Update+on+CVE-2014-6271%3A+Vulnerability+in+bash+%28shellshock%29/18707

ZDnet - Unix/Linux Bash: Critical security hole uncovered:

http://www.zdnet.com/unixlinux-bash-critical-security-hole-uncovered-7000034021/

Security Blog - Bash specially-crafted environment variables code injection attack

https://securityblog.redhat.com/2014/09/24/bash-specially-crafted-environment-variables-code-injection-attack/

Credits

Thanks to the REN-ISAC Technical Advisory Group [2] for assistance in assembling this notification, and to REN-ISAC members for valuable shared information.

References

[1] http://www.ren-isac.net

[2] http://www.ren-isac.net/about/advisory.html#technical

We'd appreciate your input on additional means to protect from the threat and general feedback concerning this Alert. If you have any questions, please don't hesitate to e-mail us at soc@ren-isac.net.

Sincerely,

Your REN-ISAC Team

http://www.ren-isac.net

24x7 Watch Desk +1(317)278-6630