Special Alert: Responding to Shellshock Vulnerability

Published on Alvarez & Marsal (https://www.alvarezandmarsal.com)

The recently disclosed vulnerability, nicknamed “Shellshock” (CVE–2014–6271 and CVE–2014–7169), in the GNU bourne again shell (Bash), affects an estimated 500 million Linux, Mac OS X, and other Unix–based systems that come with the Bash shell installed by default. In addition, this vulnerability may affect network equipment and embedded devices such as routers, firewalls and wireless access points.

The flaw involves the Bash shell executing commands that are sent to the vulnerable server in the form of environment variables. In some cases, the vulnerability can be exploited from outside your network, which can lead to system compromise. These types of cases tend to be limited to those situations where a remotely accessible server uses the Bash environment for processing user input. This may occur in some web servers that use CGI scripts to process data, or other system services such as secure shell (SSH) and dynamic host configuration protocol (DHCP) where the local Bash shell accepts environment variables from remote systems.

For many versions of Linux systems, a patch has been released that addresses this vulnerability, and it is anticipated that additional patches will be released in the coming days.

Taking Immediate Action

Although this current patch is not perfect, it does make exploiting the vulnerability more difficult. Alvarez & Marsal (A&M) recommends that this patch be applied immediately, with priority given to those servers which are Internet–facing and accepting input from remote users. Vendors of embedded systems and network equipment should be contacted in order to determine whether or not this vulnerability affects network equipment devices that may be installed on your network.

Many vulnerability and web application scanning vendors have released signatures to scan for and detect this vulnerability on systems. A&M advocates that users conduct in–depth scanning in order to determine their level of risk exposure. Where vulnerability exists and no patch is available, we recommend immediately disabling the affected service(s) on the vulnerable systems.

Finally, A&M is seeing evidence of scanning and exploitation of this vulnerability over the Internet. Many Intrusion Detection System vendors have released signatures to detect and even block exploitation attempts. We urge organizations to update their IDS signatures immediately to detect and respond to any exploitation attempts.

Key Contacts:

Art Ehuan [2]
Managing Director
+1 571 331 7763

Ryan Johnson
Director
+1 919 210 8634

For More Information:
Disputes and Investigations [3]

Source URL: https://www.alvarezandmarsal.com/insights/special-alert-responding-shellshock-vulnerability

Links

[1] https://www.alvarezandmarsal.com/insights/special-alert-responding-shellshock-vulnerability
[2] http://beta.alvarezandmarsal.com/our-people/art-ehuan
[3] http://beta.alvarezandmarsal.com/expertise/disputes-investigations