3501 Fairfax Drive • Room B7081a • Arlington, VA 22226-3550 • (703) 516-5588 • FAX (703) 562-6446 • http://www.ffiec.gov

Bourne-Again Shell (Bash) 'Shellshock' Vulnerability Alert

PURPOSE

The Federal Financial Institutions Examination Council (FFIEC) members[1] are advising financial institutions of a material security vulnerability in the Bourne-again shell (Bash) system software widely used in servers and other computing devices that could allow attackers to access and gain control of operating systems. The vulnerability, nicknamed "Shellshock," could expose organizations and individuals to potential fraud, financial loss, or access to confidential information. Given the widespread use of Bash and the evolving nature of the risk, this statement outlines FFIEC member agencies' risk mitigation expectations and provides references for management to monitor the changing threat and vulnerability landscape.

BACKGROUND

Bash is a software tool found on many operating systems[2] and is used to translate user instructions and other inputs into machine-readable commands. Financial institutions may have Bash present on a wide array of servers and network devices, including Web servers, e-mail servers, and physical security systems. On September 24, 2014, security researchers reported the existence of Shellshock in Bash versions 1.14 through 4.3, which have been in use for decades.

RISKS

The vulnerability potentially allows a remote attacker to run malware, or malicious code, on affected systems. Given the broad use of the Bash software tool, the vulnerability may be present in financial institutions', customers', and third-party service providers' systems. Attackers could use the vulnerability to access and take control of systems, leading to a range of operational risks. These risks may include the loss of confidentiality, integrity, and availability of sensitive customer information and confidential business data. Additionally, such access could facilitate data destruction, disruption of operations, and fraud.

RISK MITIGATION

While vendors are working to patch and update their systems, the FFIEC member agencies expect financial institutions to conduct a risk assessment and address the Shellshock

[1] Board of Governors of the Federal Reserve System, Consumer Financial Protection Bureau, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, and State Liaison Committee.

[2] While predominantly found on UNIX, Linux, and Mac operating systems, Bash also can be installed on Windows servers.

vulnerability as part of ongoing information security and incident response plans. Financial institutions should take the following steps, as appropriate:

- Identify all servers, systems, and appliances that use vulnerable versions of Bash and follow appropriate patch management practices, including conducting a vulnerability scan to detect if the patch is installed and testing to ensure a secure and compatable configuration.[3]
- Apply mechanisms to filter malicious traffic to vulnerable services such as appropriate Web application firewall signatures.
- Monitor systems for malicious or anomalous activity and update signatures for intrusion detection and prevention systems.
- Ensure that all third-party service providers are taking appropriate action to identify and mitigate risk and monitor the status of vendors' efforts to address the vulnerability.
- Review systems to determine if this vulnerability has been exploited and, if necessary, conduct a forensic examination to determine the potential effects of any breach.

Financial institutions are encouraged to establish mechanisms for obtaining threat and vulnerability information such as through the United States Computer Emergency Readiness Team (US-CERT) portal at www.us-cert.gov or through the Financial Services Information Sharing and Analysis Center (FS-ISAC) at www.fsisac.com.

REFERENCES

"Bourne-Again Shell (Bash) Remote Code Execution Vulnerability" (CVE-2014-6271 and CVE-2014-7169)
www.us-cert.gov/ncas/current-activity/2014/09/24/Bourne-Again-Shell-Bash-Remote-Code-Execution-Vulnerability

FFIEC Information Technology Examination Handbook, "Development and Acquisition"
http://ithandbook.ffiec.gov/it-booklets/development-and-acquisition.aspx

FFIEC Information Technology Examination Handbook, "Information Security"
http://ithandbook.ffiec.gov/it-booklets/information-security.aspx

FFIEC Information Technology Examination Handbook, "Operations"
http://ithandbook.ffiec.gov/it-booklets/operations.aspx

[3] Patch management, software maintenance, and security update practices are covered by a number of *FFIEC Information Technology Examination Handbooks,* including "Development and Acquisition," "Information Security." and "Operations."