PCI Security Standards Council

Payment Card Industry
Security Standards Council, LLC

401 Edgewater Place, Suite 600
Wakefield, MA 01880
Phone: 781 876 8855

PCI SSC Bulletin on "Shellshock" Vulnerability

15 October 2014

URGENT Immediate Action required:

The United States Department of Homeland Security via its Computer Emergency Readiness Team (US-CERT) issued a technical alert on 25 September 2014 warning organizations about a critical software vulnerability dubbed as "Shellshock" that poses a serious risk to computer systems. "Shellshock" takes advantage of a flaw in computer code in GNU Bourne-Again Shell (Bash), commonly used software that runs on UNIX-based operating systems, such as Linux and Apple's Mac OS X, making these systems potentially vulnerable to large scale compromise. Because Bash is widely used and the exploit is easily executed, "Shellshock" is especially dangerous.

The PCI Security Standards Council urges organizations to consider the following recommendations for identifying and mitigating this vulnerability that could impact the security of sensitive payment card data:

- Work with your IT departments and/or partners to identify all servers, systems, and appliances that use vulnerable versions of Bash, per Vulnerability Note VU#252743
- Review the recommendations outlined in Alert (TA14-268A) and work closely with your IT providers and partners to implement these steps as soon as possible
- Ensure proper implementation of security risk mitigating controls outlined in PCI Data Security Standard (PCI DSS) 3.0, specifically:
    - Review of public-facing web applications via manual or automated application vulnerability security assessment tools or methods, such as a web application firewall (WAF), to ensure these applications are protected against known attacks – Requirement 6.6
    - Patching of vulnerable systems, including conducting a vulnerability scan to determine if the appropriate patches are properly installed and effective – Requirements 6.2,11.2
    - Monitoring of systems for malicious and abnormal activity and updating signatures for intrusion detection and prevention systems (IDS/IPS) – Requirements 10, 11
    - Review of third-party service provider relationships, including access to devices and systems, and specifically remote access from outside an organization's network, and ensuring that partners are addressing all known vulnerabilities – Requirements 8, 12

The PCI Council reminds all organizations that a multi-layered approach to payment card security that addresses people, process and technology is critical in detecting and protecting against emerging attacks and vulnerabilities, such as "Shellshock." A daily coordinated focus on maintaining the controls outlined in the PCI Standards – making payment card security a business as usual practice - provides a strong defense against data compromise.

Additional Resources

Further details are provided in the following alerts:

- Vulnerability Note VU#252743: http://www.kb.cert.org/vuls/id/252743
- Alert (TA14-268A): https://www.us-cert.gov/ncas/alerts/TA14-268A
- Visa Security Alert: "Shellshock" Bash Vulnerability: http://usa.visa.com/download/merchants/Alert-Shellshock-100114.pdf
- Federal Financial Institutions Examination Council (FFIEC) Bourne-Again Shell (Bash) 'Shellshock' Vulnerability Alert: http://www.ffiec.gov/press/PDF/FFIEC_JointStatement_BASH_Shellshock_Vulnerability.pdf