# VISA SECURITY ALERT

**September 2014**

# "SHELLSHOCK" (BASH) VULNERABILITY

**Distribution:** Merchants, Acquirers, Issuers, Processors
**Who should read this:** IT, Information Security, and Risk Management

## Summary

On Wednesday, September 24, the Financial Services Information Sharing and Analysis Center (FS-ISAC) reported on "Shellshock", a newly discovered security vulnerability in Unix-based operating systems such as Linux and Apple's Mac OS X.

## Gnu Bourne-Again Shell (BASH) "Shellshock" Vulnerability

Security researchers announced the discovery of a critical exploit in Bash, a command line shell common in UNIX and Linux operating systems. The vulnerability has existed for more than 20 years but was only discovered recently. Bash can be found in most Linux iterations as well as appliances, networking devices, firewalls, Mac OS X, etc. Bash can be invoked by Apache via CGI, as well as SSH, telnet and other common services and programs. Some researchers and media outlets are referring to this vulnerability as "Shellshock."

The vulnerability is remotely exploitable and can allow arbitrary code execution on vulnerable systems. Exploit code for Shellshock has already been incorporated into Metasploit, a common hacking tool. It is possible that hackers will use the vulnerability to create a worm that automatically spreads from vulnerable machine to vulnerable machine. The result would be a botnet, a network of thousands of compromised machines that operate under the control of a single hacker. These botnets — which are often created in the wake of major vulnerabilities — can be used to send spam, participate in denial-of-service attacks on websites or to steal confidential data.

## Mitigation

Visa recommends that clients using Linux and Mac OS X systems determine if their version of Bash is vulnerable, and immediately apply the security update to vulnerable systems. As of this publication, most major Linux distributions have released an update that may be applied using the distribution's package management system.

Some are recommending that users check whether or not they are running CGI – but that is absolutely not enough. C++, Python, PHP and all other applications that make Bash calls are affected. Other applications supporting DHCP, SSH (restricted shell) may also be affected, not only from a remote attack but also from a local privilege escalation perspective.

All participants in the payments system 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 compatible configuration.
- Apply mechanisms to filter malicious traffic to vulnerable services such as appropriate Web application firewall (WAF) signatures.
- Monitor systems for malicious or anomalous activity and update signatures for intrusion detection and prevention systems (IDS/IPS).
- 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.

## Additional Resources

Further details are provided in the US-CERT alert
https://www.us-cert.gov/ncas/alerts/TA14-268A

Mitigating the shellshock vulnerability (CVE-2014-6271 and CVE-2014-7169)
https://access.redhat.com/articles/1212303

Core Security - Bash Bug, Shellshock, CVE-2014-6271
http://blog.coresecurity.com/2014/09/25/bash-bug-shellshock-cve-2014-6271/

**To report a data breach, contact Visa Fraud Control:**

- Asia Pacific Region, Central Europe/Middle East/Africa Region: VIFraudControl@visa.com
- Canada Region, Latin America Region, United States: USFraudControl@visa.com

For more information, please contact Visa Risk Management: cisp@visa.com