Payment Card Industry
Security Standards Council, LLC

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

PCI SSC Bulletin on "GHOST" Vulnerability

2 February 2015

URGENT Immediate Action required:

On 27 January the United States Department of Homeland Security via its Computer Emergency Readiness Team (US-CERT) warned organizations about a critical software vulnerability dubbed as "GHOST" that poses a serious risk to computer systems. "GHOST" affects Linux GNU C Library (glibc) versions prior to 2.18. Hackers can exploit this vulnerability via a remote code execution, which can enable them to take control over the impacted system and wreak havoc by potentially deleting files, installing malware and any other activity that can be done via stolen credentials.

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 glibc.
- Organizations that determine they are running vulnerable Linux versions should:
  - Review the recommendations outlined in Vulnerability Note VU#967332.
  - Work closely with your IT departments and/or providers and partners to obtain the appropriate patch from your vendor - all Linux distribution vendors have patches available to address this vulnerability.
  - Implement the patch as soon as possible.

In addition, to address these types of risks going forward, organizations should ensure proper implementation of security risk mitigating controls outlined in PCI Data Security Standard (PCI DSS) 3.0, specifically:

- Review of public-facing web application activity via vulnerability security assessment tools or methods, such as a web application firewall (WAF), to ensure these applications are protected against known attacks and operating as expected – Requirement 6.6
- Patching of vulnerable systems, including conducting quarterly vulnerability scans 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 "GHOST." 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#967332: http://www.kb.cert.org/vuls/id/967332
- US-CERT: https://www.us-cert.gov/ncas/current-activity/2015/01/27/Linux-Ghost-Remote-Code-Execution-Vulnerability
- MITRE CVE entry: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0235