January 27, 2015

Qualys Releases Security Advisory for "GHOST" Vulnerability on Linux Systems

High Severity Vulnerability Found in Linux GNU C Library Gives Attackers Control Without System Credentials; Patches Available Today

REDWOOD CITY, CA -- (Marketwired) -- 01/27/15 -- Qualys, Inc. (NASDAQ: QLYS), a pioneer and leading provider of cloud security and compliance solutions, today announced that its security research team has found a critical vulnerability in the Linux GNU C Library (glibc), that allows attackers to remotely take control of an entire system without having any prior knowledge of system credentials. Qualys has worked closely with Linux distribution vendors in a coordinated effort to offer a patch for all distributions of Linux systems impacted, which is available today from the corresponding vendors.

The vulnerability known as GHOST (CVE-2015-0235) as it can be triggered by the gethostbyname functions, impacts many systems built on Linux starting with glibc-2.2 released on November 10, 2000. Qualys researchers also identified a number of factors that mitigate the impact of this bug including a fix released on May 21, 2013 between the releases of glibc-2.17 and glibc-2.18. Unfortunately, this fix was not classified as a security advisory, and as a result, most stable and long-term-support distributions were left exposed including: Debian 7 (wheezy), Red Hat Enterprise Linux 6 & 7, CentOS 6 & 7 and Ubuntu 12.04.

Qualys customers can detect GHOST by scanning with the Qualys Vulnerability Management (VM) cloud solution as QID 123191. This means that Qualys customers can get reports detailing their enterprise-wide exposure during their next scanning cycle, which allows them to get visibility into the impact within their organization and efficiently track the remediation progress of this serious vulnerability.

"GHOST poses a remote code execution risk that makes it incredibly easy for an attacker to exploit a machine. For example, an attacker could send a simple email on a Linux-based system and automatically get complete access to that machine," said Wolfgang Kandek, Chief Technical Officer for Qualys, Inc. "Given the sheer number of systems based on glibc, we believe this is a high severity vulnerability and should be addressed immediately. The best course of action to mitigate the risk is to apply a patch from your Linux vendor."

For more information on GHOST including a podcast, follow the conversation on our Laws of Vulnerabilities blog.

Additional Resources

- Learn more about Qualys Vulnerability Management
- Follow Qualys on LinkedIn and Twitter

About Qualys, Inc.
Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud security and compliance solutions with over 6,700 customers in more than 100 countries, including a majority of each of the Forbes Global 100 and Fortune 100.The Qualys Cloud Platform and integrated suite of solutions help organizations simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for IT systems and web applications. Founded in 1999, Qualys has established strategic partnerships with leading managed service providers and consulting organizations including Accenture, Accuvant, BT, Cognizant Technology Solutions, Dell SecureWorks, Fujitsu, HCL Comnet, InfoSys, NTT, Tata Communications, Verizon and Wipro. The company is also a founding member of the Cloud Security Alliance (CSA) and Council on CyberSecurity. For more information, please visit www.qualys.com.

MEDIA CONTACTS:
Melissa Liton
Qualys, Inc.
(650) 801-6242
Email Contact

Michelle Kincaid

LEWIS PR on behalf of Qualys
(415) 432-2467
Email Contact

Source: Qualys