New Linux Vulnerability in GNU C Library (glibc) – Nicknamed ‘Ghost’

CVE-2015-0235

GHOST gethostbyname() heap overflow in glibc
GHOST glibc gethostbyname buffer overflow

Summary:

A new buffer overflow vulnerability has been found in the gnu c library (glibc) which is found in all Linux systems. It is being referred to publicly as the ‘Ghost’ vulnerability. The buffer overflow would allow for the execution of arbitrary code both remotely and potentially even locally. The vulnerability was patched on 2013-05-21 but was not marked as a security vulnerability and thereby may not have been applied by system administrators.

What’s Vulnerable?

All versions of glibc from: glibc-2.2 (released 2010-11-10) until glibc-2.17 are vulnerable.

EXIM MTA as there is a PoC (proof-of-concept) code currently available for exploitation.

Severity:

Urgent

What To Do?

Please install vendor or version specific patches so only glibc-2.18 version or later is in use.

RESTART – It is imperative to restart the system after patching in order for the changes to take effect.

What Does This Affect?

All Linux systems.

References:

NIST National Vulnerability Database: CVE-2015-0235

CERT Vulnerability Notes Database:
http://www.kb.cert.org/vuls/id/967332

Red Hat Customer Portal:
https://access.redhat.com/articles/1332213

Qualys – Original research documentation and notification: