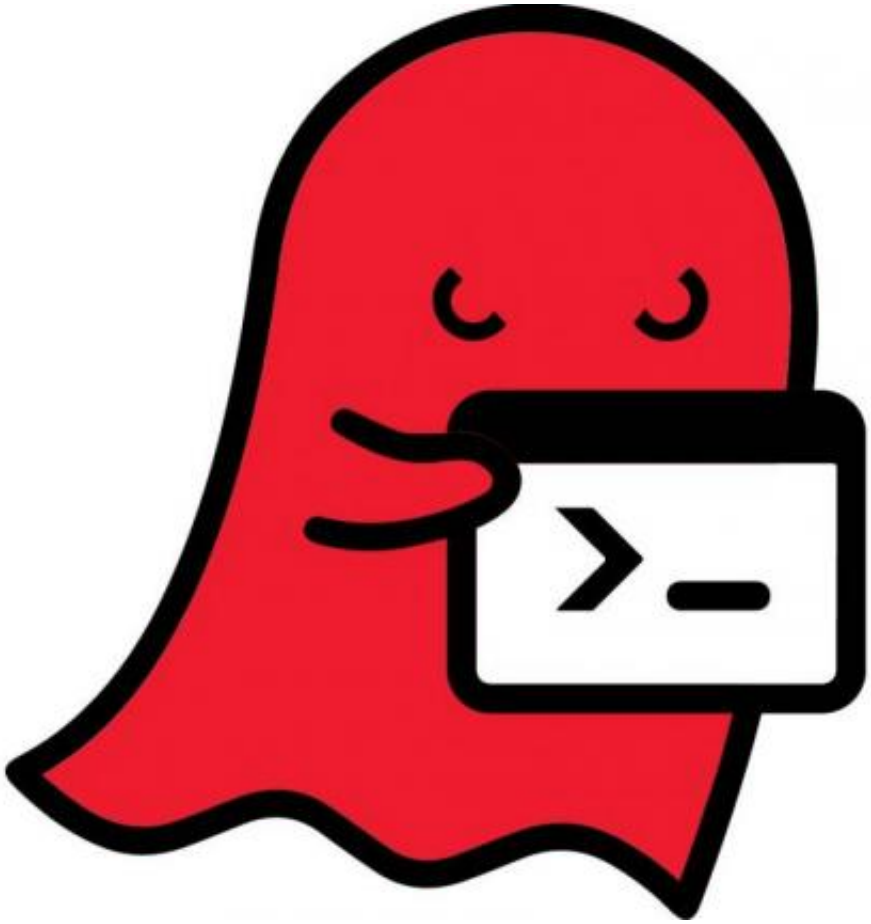
Linux distrib vendors make patches available for GHOST

January 29 2015, by Nancy Owano



Qualys said on Tuesday that there was a serious weakness in the Linux glibc library. During a code audit, Qualys researchers discovered a

buffer overflow in the __nss_hostname_digits_dots() function of glibc. The weakness can allow attackers to remotely take control of the victim's system without any prior knowledge of system credentials. This has become known as the GHOST vulnerability, discovered by researchers at the security company Qualys, which worked closely with Linux distribution vendors.

The company also thanked Alexander Peslyak of the Openwall Project for his help with the disclosure process. (Peslyak has been professionally involved in computer and network security since 1997.) The Openwall Project is a source for various software. Amol Sarwate, Qualys Vulnerability Labs Director, served as the presenter in a video explaining the company's advisory. He said the weakness was serious but patches were available from Linux distributions, he added, in the Tuesday posting. What is "glibc"? This is the Gnu C library and a core part of the OS. "The vulnerability is in one of the functions of glibc," said Sarwate, where a buffer overflows.The vulnerability can be triggered locally and remotely from any of the gethostbyname*() functions.

So what's the risk? An attacker, said Sarwate, could send a malicious email to an email server and get a remote shell to the Linux machine. The good news is that most Linux vendors have released patches. "So the best way to mitigate this issue," said Sarwate, "is to apply a patch from your Linux distribution."

Gavin Millard, technical director of Tenable Network Security, told the *Telegraph*: "Patches are being released for the major Linux distributions and should be applied with a priority on any vulnerable systems with services that can be reached from the Internet."

Sarwate said the vulnerability is called "GHOST" because of the GetHOST functions by which the flaw can be exploited. The vulnerability has a history; it was found some years ago and it was fixed

but it was not classified as a security vulnerability. Nonetheless, as of Tuesday, distributions have released patches, said Sarwate, "so please install patches for your servers."

Dan Goodin of *Ars Technica* had some words of caution: "patching systems requires core functions or the entire affected server to be rebooted, a requirement that may cause some systems to remain vulnerable for some time to come." Goodin called the vulnerability "extremely critical."

The GNU C Library (glibc) is primarily designed to be a portable and high-performance C library. Any Unix-like operating system needs a C library: the library which defines the ``system calls'' and other basic facilities. The GNU C Library is used as the C library in GNU systems and most systems with the Linux kernel. It follows all relevant standards including ISO C11 and POSIX.1-2008. It is also internationalized.

Jeremy Kirk of the IDG News Service made note that this is "one of many issues found over the last year in open-source software components, including Heartbleed, Poodle and Shellshock, that have caused alarm due to the large number of systems affected."

More information: — community.qualys.com/blogs/law … -ghost-vulnerability
— www.qualys.com/research/securi … ST-CVE-2015-0235.txt