Digi International Security Notice Vulnerability "GHOST"

Digi International Security Notice

March 6th, 2015

CVE-2015-0235

Overview

A critical security vulnerability, reported as CVE-2015-0235, nicknamed "GHOST," was discovered by Qualys. The vulnerability affects the GetHostbyName API call within the GNU libc libraries. Virtually all programs written under UNIX and in the C language use this library. The purpose of this notice is to inform you of the vulnerability, how it affects Digi products, and the possible steps necessary to remediate this issue. In our testing of this vulnerability, we found that there was not a single case where a remote attacker could gain unauthorized access to your device. Further, we have rated this vulnerability as LOW/NON Exploitable risk to our customers.

Affected Products

The security teams at Digi has evaluated the exposure of the vulnerability to Digi products and determined the overall risk to this vulnerability to our products is low. We have found that a small number of our products contain the glibc vulnerable libraries, of which none are remotely exploitable. The following products are impacted:

- Digi CM
- ConnectPort X2e

Following best security practices, Digi will review and patch the existing libraries within these products during its normal release cycles. Digi recommends to all of its customers to update their products firmware versions on a periodic basis.

Products Not Affected

The following Digi products and services are not affected by this vulnerability:

- Connect WAN, WAN 3G, ES, SP/Wi-SP, N2S
- ConnectPort X2, X4, X4H, X5, WAN, TS
- NET+OS
- PortServer TS
- Anywhere USB
- TransPort WR11, WR21, WR41, WR44
- NET+OS
- Device Cloud by Etherios
- Cloud Connector by Etherios
- Rabbit
- www.digi.com Website

Note: If you have any questions on any Digi products and services that are not listed, please contact us at +1 (952) 912-3456, or via the web site at www.digi.com/support.

Detailed Information on Affected products

Background

The vulnerability, which started officially as CVE-2015-0235, and nicknamed “GHOST”, initially seems to have the potential to impacted many different applications on the Internet. This vulnerability is based in the deep common code libraries (GNU libc) that virtually all programs use to interact on the systems that they run on. The specific call, GetHostbyName OS call converts Internet names to the actual numbers needed to route data between networked systems. This means that any program that a user inputs a name like www.digi.com, could be vulnerable. This name can be passed to the glibc call that has been impacted.

It turns out that the glibc libraries that are impacted started with glibc-2.2 (released on Nov, 10th 2000), and ended on glibc-2.18 (released on May, 21st 2013) the initial fix in 2013 was done for other reasons, and was NOT initially identified as a security threat at that time.

Digi maintains a security team that will continue to review new results as they are found from this threat, and test our solutions and products for any new and emerging security vulnerabilities. Security is a top priority and something we take very seriously.

Analysis

We have used various commercial scanners, as well as manual methods to conduct these tests and determine our results. For GHOST, testing for this exploit comes in the form of validating all end user input into our products. Since we conduct this testing on a standard basis for all of our products upon release, there have been no results found that could be related to this vulnerability. Further, for the products that may rely on the vulnerable libraries, these programs have limited network end user input. The initial analysis of this vulnerability was rated high since so many programs on traditional UNIX systems use these libraries. The initial expectations were that many programs would be susceptible to this bug. However, at this time, there are only 4 programs that have been found to be vulnerable. Those programs are EXIM (a UNIX mailer), clockdiff, pppd, procmail (comsat/biff feature). Further, it was found to be difficult to conduct the necessary 1024 character input needed to trigger the glibc vulnerability, as there are other input validation systems in place that would block this from being exploited.

Below is our analysis of the threat, the risk of what may be exposed, and how we recommend our customers mitigate the threat.

Functions impacted:

- No functions have been found to be impacted by this vulnerability.

Functions NOT impacted:

We believe that all functions with our devices and software are not affected by this. This vulnerability requires a vulnerable program that depends on vulnerable glibc library. Since Digi routinely reviews and test end user submitted fields and data in our programs, we are not aware of any place where both errors exist to allow this vulnerability to be executed.

Risk

For generic risks of this vulnerability, see the links below. For specific risks to Digi international products, we have classified the risk of GHOST to our products as ***VERY LOW/ NON Exploitable***. During our testing, we were not able to find any remote exploits from this vulnerability. Further, we were not able to find any locations where a privilege escalation could become an issue. For each product tested, and where we identified the

glibc library as being affected, at a minimum, an attacker would need to have full access to the device for the exploit. Assuming that any program was affected, a privilege escalation would not be possible.

During the testing, we did not see a single place where we were impacted. Although US-CERT has rated this vulnerability as the highest (CVSS of 10.0), the real threat with our devices are significantly much lower. Below are the reasons for this:

Risk of GHOST to our products and services are:

- The initial review of GHOST was that the network was the Access Vector. For our devices we do not run any of the known vulnerable programs with network access.
- None of the local programs that were impacted are installed on our systems.
- No user privileged escalation path has been identified in any of the GHOST vulnerabilities. In the case of a hypothetical local exploit, getting a working local exploit would gain you nothing but full access to a system you already had full access to.
- We routinely test user input scenarios into our programs and validate that they do not overflow. Since our devices only have a limited set of functions, the threat is considered much lower than if it was a full blown Linux server with much more “attack surface” where a glibc exploit could be found.
- Our products do not offer a build environment on the product, so adding any additional code to the device requires at a minimum, access as a full access user.

Risk needs to be determined by the end customer and how they have chosen to deploy the device within their environment. We make this determination based on the following criteria:

- Most customers have deployed the devices within a network that is not reachable from the Internet.
- The vulnerability is not remotely exploitable. For each case tested, we believe that full access to the device is needed to even see the vulnerability.

Suggested Steps to Protect Your Devices

Although we have rated this as non-impacting to any Digi devices, we still suggest the following steps.

Mitigation Steps

Check this notice for firmware release versions and dates. You can also visit www.digi.com/support for more information specific to your device. We would also recommend subscribing to the RSS feed on the support site for your product to get immediate notice of any new firmware or document releases specific to your product.

If a firmware update is not available, we currently do not have any further recommendations to mitigate this vulnerability. If you believe that a feature of your device is at risk, we invite you to contact us further.

Resources for GHOST

If you are interested in learning more about the disclosure, please feel free to visit the web pages below:

- Trendmicro Labs – Not So Spooky: Linux "Ghost" Vulnerability – http://blog.trendmicro.com/trendlabs-security-intelligence/not-so-spooky-linux-ghost-vulnerability/
- Qualys Blog - https://community.qualys.com/blogs/laws-of-vulnerabilities/2015/01/27/the-ghost-vulnerability
- Tech Radar - http://www.techradar.com/us/news/software/security-software/all-you-need-to-know-about-the-ghost-vulnerability-1282919
- Sucuriblog technical info - http://blog.sucuri.net/2015/01/critical-ghost-vulnerability-released.html
- Don't be shellshocked by GHOST - http://www.tripwire.com/state-of-security/vulnerability-management/dont-be-shellshocked-by-ghost/

If you have any other questions regarding this vulnerability and how it affects Digi hardware products and the Digi Device Cloud products, feel free to contact us at security@digi.com.