Hewlett Packard Enterprise

HPE Software Security Update

HPE Connect-It and the CVE-2015-7547 glibc getaddrinfo Stack-Based Buffer Overflow Vulnerability

Document management:

Date	Version	Change
March 04, 2016	Version 1.0	Initial release

Summary:

The following article provides information regarding CVE-2015-7547, known as the glibc getaddrinfo Stack-Based Buffer Overflow Vulnerability and Hewlett Packard Enterprise (HPE) Connect-It.

Topic:

CVE-2015-7547

https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-7547

https://security.googleblog.com/2016/02/cve-2015-7547-glibc-getaddrinfo-stack.html

Note: *These links provide detailed background information about this issue.*

The Linux GNU C library (glibc) exposes new vulnerabilities as described in CVE-2015-7547. The glibc DNS client side resolver is vulnerable to a stack-based buffer overflow when the `getaddrinfo` library function is used. Software using this function may be exploited with attacker-controlled domain names, attacker-controlled DNS servers, or through a man-in-the-middle attack.

Affected Releases:

The following versions of HPE Connect-It (CIT) were found vulnerable.

- All Connect-It versions running on Linux platforms with a glibc version of 2.9 to 2.22

ACTION: Review all details in the instructions provided in this article to address the vulnerability.

HPE recommends all Connect-It customers evaluate this information and take action as soon as possible.

Response:

Impact on Connect-It

Connect-It (CIT) does not ship or bundle the glibc library in its deliverable components. Instead CIT dynamically links to the glibc and as a result, when Connect-It runs, it uses the underlying operating system's default glibc library. If the version of your operating system's glibc is 2.9 to 2.22, you may be vulnerable to CVE-2015-7547.

Mitigation Actions

Hewlett Packard Enterprise recommends that affected systems running Connect-It immediately upgrade their operating system's glibc library to version 2.23 as recommended by the CVE identifier listed in the Topic section of this document. Please consult with your operating system's system administrator for details on properly updating the glibc library. As HPE does not provide or ship the glibc library, upgrading it is the responsibility of the customer.