SSA-301706: GNU C Library Vulnerability in Industrial Products

Publication Date 2016-04-08
Last Update 2016-09-22
Current Version V1.3
CVSSv3 Base Score 8.1

SUMMARY

The glibc vulnerability CVE-2015-7547 [1] affects several Siemens industrial products. The vulnerability could potentially allow attackers to cause a Denial-of-Service of the affected products or to execute arbitrary code under certain conditions.

Siemens provides updates for all affected products.

AFFECTED PRODUCTS

The following products are affected in their default configuration:

- ROX II: V2.3.0 - V2.9.0 (inclusive)
- APE (Linux) : All versions
- SINEMA Remote Connect: All versions < V1.2
- SCALANCE M-800 / S615: All versions < V4.02
- Basic RT V13: All versions < V13 SP1 Update 9

DESCRIPTION

Vulnerability CVE-2015-7547 in GNU C Library (glibc) affects several Siemens industrial products. The vulnerability could potentially allow attackers to cause a Denial-of-Service of the affected products or to execute arbitrary code under certain conditions.

Detailed information about the vulnerability is provided below.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3 (CVSSv3) (http://www.first.org/cvss/). The CVSS environmental score is specific to the customer's environment and will impact the overall CVSS score. The environmental score should therefore be individually defined by the customer to accomplish final scoring.

Vulnerability Description (CVE-2015-7547)

A stack-based buffer overflow vulnerability (CVE-2015-7547) has been identified in glibc. The vulnerability occurs within the library's DNS client side resolver and could allow an attacker to cause a Denial-of-Service of the affected device or to execute arbitrary code on the affected device.

CVSS Base Score 8.1
CVSS Vector CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C

Mitigating Factors

In order to exploit the vulnerability, the attacker must be able to either trick a targeted host to resolve attacker-controlled domain names, to use attacker-controlled DNS servers for resolution, or to gain a privileged network position allowing him to capture and modify the affected device’s network communication.

Siemens recommends operating non-perimeter devices only within trusted networks [7].

SOLUTION

Siemens provides updates for the following products and encourages customers to update their products:

- ROX II: Update to version 2.9.1 [2]
- APE (Linux): Follow update process provided in the corresponding application note [3]
- SINEMA Remote Connect: Update to version 1.2 [4]
- Basic RT V13: Update to Version V13 SP 1 Update 9 [5]
- SCALANCE M-800 / S615: Update to V4.02 [6]

Siemens recommends applying the following mitigations until patches can be applied:

- Disable use of DNS on affected devices if possible, or
- Use of trusted DNS servers, trusted networks/providers, and known trusted DNS domains in device configuration, or
- Limit size of DNS responses to 512 bytes for UDP messages, and 1024 bytes for TCP messages on network border

As a general security measure Siemens strongly recommends to protect network access to non-perimeter devices with appropriate mechanisms. It is advised to configure the environment according to our operational guidelines [7] in order to run the devices in a protected IT environment.

ADDITIONAL RESOURCES

[1] Further information on the glibc vulnerability (CVE-2015-7547):
https://googleonlinesecurity.blogspot.de/2016/02/cve-2015-7547-glibc-getaddrinfo-stack.html

[2] The firmware updates for the affected ROX-based products can be obtained from the following contact points:
  - o Submit a support request online
    https://www.siemens.com/automation/support-request
  - o Call a local hotline center:
    https://w3.siemens.com/aspa_app/

[3] The APE (Linux) application note can be obtained from:
http://support.automation.siemens.com/WW/view/en/109485761

[4] The software update for SINEMA Remote Connect can be obtained from:
https://support.industry.siemens.com/cs/ww/en/view/109737963

[5] The software update for Basic RT V13 can be obtained from:
https://support.industry.siemens.com/cs/ww/en/view/109311724

[6] Firmware update V4.02 for Scalance M-800 / S615 can be obtained for free from:
https://support.industry.siemens.com/cs/ww/en/view/109740858

[7] An overview of the operational guidelines for Industrial Security:
https://www.siemens.com/cert/operational-guidelines-industrial-security

[8] Information about Industrial Security by Siemens:
https://www.siemens.com/industrialsecurity

[9] For further inquiries on vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:
https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2016-04-08): Publication Date
V1.1 (2016-06-08): Added patch information for SINEMA Remote Connect
V1.2 (2016-07-12): Added patch information for Basic RT V13
V1.3 (2016-09-22): Added patch information for Scalance M-800 / S615

DISCLAIMER