SSA-994726: GHOST Vulnerability in Siemens Industrial Products

Publication Date: 2015-03-05
Last Update: 2020-02-10
Current Version: V1.2
CVSS v3.1 Base Score: 5.5

SUMMARY

The latest updates for the affected products fix the “GHOST” [1] vulnerability identified in glibc library (CVE-2015-0235).

Incorrect parsing within the glibc library functions “gethostbyname()” and “gethostbyname2()” could cause a Denial-of-Service of the targeted system.

[1] https://nvd.nist.gov/vuln/detail/CVE-2015-0235

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Ruggedcom APE1402-XX, APE1402-C01, APE1404-XX, APE1404-C01: All versions	These products are not exploitable in the default configuration. If a vulnerable software component is installed and users configure the system in a certain way, it may become exploitable. Follow update process provided in the corresponding application note: https://support.industry.siemens.com/cs/ww/en/view/109474273
SIMATIC HMI Basic Panels 2nd Generation (incl. SIPLUS variants): All versions	Update 2 for SIMATIC WinCC (TIA Portal) V13 SP1 https://support.industry.siemens.com/cs/ww/en/view/109311724
SINUMERIK 808D, 828D, 840D sl: All versions <= V4.7	For version V2.7:update to V2.7 SP4 Hotfix 3; For version V4.5:update to V4.5 SP4 Hotfix 4; For version V4.7:update to V4.7 SP1 The update for SINUMERIK can be obtained from your local Siemens account manager.

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- For the affected SINUMERIK controllers and SIMATIC HMIs, restrict local access to the device.
- For Ruggedcom APE, the attacker must be able to influence parameters that are passed to the vulnerable functions. This is only possible if the user installed applications on the device which use the vulnerable functions, and if those functions are accessible by an attacker. Follow the process provided in the corresponding remediation table.

GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens' operational guidelines for Industrial Security (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security), and to follow the recommendations in the product manuals.

Additional information on Industrial Security by Siemens can be found at: https://www.siemens.com/industrialsecurity

PRODUCT DESCRIPTION

SINUMERIK CNC offers automation solutions for the shop floor, job shops and large serial production environments.

RUGGEDCOM APE serves as an utility-grade computing platform for the RUGGEDCOM RX1500 router family. It also allows to run third party software applications without needing to procure an external industrial PC.

SIMATIC HMI Panels are used for operator control and monitoring of machines and plants.

SIPLUS extreme products are designed for reliable operation under extreme conditions and are based on SIMATIC, LOGO!, SITOP, SINAMICS, SIMOTION, SCALANCE or other devices. SIPLUS devices use the same firmware as the product they are based on.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.1 (CVSS v3.1) (https://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.

An additional classification has been performed using the CWE classification, a community-developed list of common software security weaknesses. This serves as a common language and as a baseline for weakness identification, mitigation, and prevention efforts. A detailed list of CWE classes can be found at: https://cwe.mitre.org/.

Vulnerability CVE-2015-0235

The vulnerability could cause a Denial-of-Service of the system. Only authenticated users may exploit this vulnerability.

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C
CWE	CWE-122: Heap-based Buffer Overflow

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Artem Zinenko from Kaspersky for pointing out that SIPLUS should also be mentioned

ADDITIONAL INFORMATION

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2015-03-05): Publication Date
V1.1 (2015-04-22): Added update for SIMATIC HMI Basic Panels 2nd Generation
V1.2 (2020-02-10): SIPLUS devices now explicitly mentioned in the list of affected products

TERMS OF USE