SSA-809841: Buffer Overflow Vulnerability in Third-Party Component pppd

Publication Date: 2020-08-11
Last Update: 2020-08-11
Current Version: V1.0
CVSS v3.1 Base Score: 9.8

SUMMARY

The latest update for SCALANCE M-800 / S615 and RUGGEDCOM RM1224 devices fixes a buffer overflow vulnerability in the third party component pppd that could allow an attacker with network access to an affected device to execute custom code on the device.

Siemens has released updates for affected devices and recommends specific countermeasures.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
RUGGEDCOM RM1224: All versions < V6.3	Update to V6.3 https://support.industry.siemens.com/cs/ww/en/view/109781070
SCALANCE M-800 / S615: All versions < V6.3	Update to V6.3 https://support.industry.siemens.com/cs/ww/en/view/109781070

WORKAROUNDS AND MITIGATIONS

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

- Only use the PPP functionality of the affected devices in trusted environments. This functionality is not enabled by default but typically used in internet dial-in or Point-to-Point connection scenarios. At this point the vulnerability could be exploited by a malicious peer.

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

The SCALANCE M-800 / S615 industrial routers are used for secure remote access to plants via mobile networks, e.g. GPRS or UMTS with the integrated security functions of a firewall for protection against unauthorized access and VPN to protect data transmission.

RUGGEDCOM RM1224 is a 4G ROUTER for wireless IP-communication from Ethernet based devices via LTE(4G)- mobile radio, optimized for use in North America.

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-2020-8597

The version of pppd shipped with this product has a vulnerability that may allow an unauthenticated remote attacker to cause a stack buffer overflow, which may allow arbitrary code execution on the target system.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

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 (2020-08-11): Publication Date

TERMS OF USE

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website (https://www.siemens.com/terms_of_use, hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.