SSA-493830: Privilege Escalation in ROX II

Publication Date: 2018-10-09
Last Update: 2018-10-09
Current Version: V1.0
CVSS v3.0 Base Score: 8.8

SUMMARY

The latest update for ROX II fixes two vulnerabilities. One vulnerability could allow an attacker with a low-privileged user account to execute arbitrary commands. The other vulnerability could allow an attacker with a low-privileged user account to escalate his privileges.

Siemens recommends to update to the new version as soon as possible.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
ROX II: All versions < V2.12.1	Update to V2.12.1 https://support.industry.siemens.com/cs/us/en/view/109760683

WORKAROUNDS AND MITIGATIONS

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

- Restrict network access to prevent potential attackers from accessing 22/tcp if possible

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

ROX-based VPN endpoints and firewall devices are used to connect devices that operate in harsh environments such as electric utility substations and traffic control cabinets.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (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.

Vulnerability CVE-2018-13801

An attacker with network access to port 22/tcp and valid low-privileged user credentials for the target device could perform a privilege escalation and gain root privileges.

Successful exploitation requires user privileges of a low-privileged user but no user interaction. The vulnerability could allow an attacker to compromise confidentiality, integrity and availability of the system.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.0 Base Score	8.8
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

Vulnerability CVE-2018-13802

An authenticated attacker with a high-privileged user account access via SSH could circumvent restrictions in place and execute arbitrary operating system commands.

Successful exploitation requires that the attacker has network access to the SSH interface in on port 22/tcp. The attacker must be authenticated to exploit the vulnerability. The vulnerability could allow an attacker to execute arbitrary code on the device.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.0 Base Score	7.2
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Gerard Harney from NCC Group for coordinated disclosure of CVE-2018-13801

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 (2018-10-09): 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.