SSA-646841: Recoverable Password from Configuration Storage in SCALANCE X Switches

Publication Date: 2019-06-11
Last Update: 2019-06-11
Current Version: V1.0
CVSS v3.0 Base Score: 7.1

SUMMARY

A vulnerability exists in the affected devices that could allow external entities to reconstruct passwords for users of the affected devices if an attacker is able to obtain a backup of the device configuration.

Siemens has released updates for some of the affected devices and is working on updates for the remaining affected products and recommends specific countermeasures until fixes are available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SCALANCE X-200: All Versions < V5.2.4	Update to V5.2.4 https://support.industry.siemens.com/cs/ww/en/view/109767965
SCALANCE X-200IRT: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X-300: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X-414-3E: All versions	migrate to SCALANCE XM400 product line

WORKAROUNDS AND MITIGATIONS

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

- Restrict access to config backups or archived device configuration files
- Restrict or disable network access to mechanisms that allow to retrieve the device configuration, if enabled.
- Restrict access to device configuration module C-PLUG, if in use.

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 (https://cert-portal.siemens.com/operational-guidelines-industrial-security.pdf), 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

SCALANCE X switches are used to connect industrial components like Programmable Logic Controllers (PLCs) or Human Machine Interfaces (HMIs).

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-2019-6567

The affected devices store passwords in a recoverable format. An attacker may extract and recover device passwords from the device configuration.

Successful exploitation requires access to a device configuration backup and impacts confidentiality of the stored passwords.

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

CVSS v3.0 Base Score	7.1
CVSS Vector	CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Christopher Wade from Pen Test Partners for coordinated disclosure

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 (2019-06-11): 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.