SSA-766247: Authentication Vulnerability in SIMATIC Process Historian

Publication Date: 2021-10-12
Last Update: 2021-10-12
Current Version: V1.0
CVSS v3.1 Base Score: 9.8

SUMMARY

The latest update for SIMATIC Process Historian (PH) fixes an authentication vulnerability in the configuration interface of redundant PH instances that could enable the execution of admin operations on the database.

The related vulnerable interface is restricted to local access on recent versions starting from SIMATIC Process Historian 2020.

Siemens has released an update for the SIMATIC Process Historian 2014 and recommends to update to the latest version. Siemens is preparing further updates and recommends specific countermeasures for products where updates are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC Process Historian 2013 and earlier: All versions	See recommendations from section Workarounds and Mitigations or upgrade to a newer SIMATIC Process Historian version
SIMATIC Process Historian 2014: All versions < SP3 Update 6	Update to SP3 Update 6 or later version https://support.industry.siemens.com/cs/ww/en/view/109780528/
SIMATIC Process Historian 2019: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC Process Historian 2020: All versions	See recommendations from section Workarounds and Mitigations

WORKAROUNDS AND MITIGATIONS

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

- Deactivate following incoming rules in the local Windows firewall:
  - PH Redundancy Services
  - PH Wcf MessageQueue Service (RedundancyMaintenanceService)
  - PH Wcf MessageQueue Service (SqlMirroringSetup)
  - PH Wcf MessageQueue Service (MaintenanceService)
  - PH SQL-Server Mirroring Port (UDP)
  - PH SQL-Server Mirroring Port (TCP)
- In case SIMATIC Process Historian is used as a redundant system, restrict remote IP addresses in the firewall rules to allow only access for the Master, the Standby and the Mirror server

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 SIMATIC Process Historian is the long term archive system for SIMATIC PCS 7, SIMATIC WinCC and SIMATIC PCS neo. It stores process values, alarms and batch data of production plants in its database and offers historical process data to reporting and visualization applications.

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-2021-27395

An interface in the software that is used for critical functionalities lacks authentication, which could allow a malicious user to maliciously insert, modify or delete data.

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-306: Missing Authentication for Critical Function

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 (2021-10-12): Publication Date

TERMS OF USE