SSA-535380: Command Injection Vulnerability in Siveillance OIS Affecting Several Building Management Systems

Publication Date: 2021-09-14
Last Update: 2021-09-14
Current Version: V1.0
CVSS v3.1 Base Score: 10.0

SUMMARY

The Siveillance Open Interface Services (OIS) application used for integration of different subsystems to several Siemens building management systems contains a command injection vulnerability that could allow a remote unauthenticated attacker to execute code on the affected system with root privileges.

Siemens has released patches and updates for Siveillance OIS to apply to the products that incorporate the OIS service, and recommends to update to the latest versions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Desigo CC: All versions with OIS Extension Module	Update the OIS to V2.5.3 or apply the patch https://support.industry.siemens.com/cs/ww/en/view/109799908/
GMA-Manager: All versions with OIS running on Debian 9 or earlier	Update the OIS to V2.5.3 or apply the patch https://support.industry.siemens.com/cs/ww/en/view/109799908/
Operation Scheduler: All versions with OIS running on Debian 9 or earlier	Update the OIS to V2.5.3 or apply the patch https://support.industry.siemens.com/cs/ww/en/view/109799908/
Siveillance Control: All versions with OIS running on Debian 9 or earlier	Update the OIS to V2.5.3 or V2.6.1, or apply the patch https://support.industry.siemens.com/cs/ww/en/view/109799908/
Siveillance Control Pro: All versions	Update the OIS to V2.5.3 or V2.6.0, or apply the patch https://support.industry.siemens.com/cs/ww/en/view/109799908/

WORKAROUNDS AND MITIGATIONS

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

- Ensure that the systems where Siveillance OIS is installed are only accessible by trusted personnel
- Restrict access to the affected systems, especially to port 443/tcp, to trusted IP addresses only

GENERAL SECURITY RECOMMENDATIONS

As a general security measure Siemens strongly recommends to protect network access to affected products with appropriate mechanisms. It is advised to follow recommended security practices in order to

run the devices in a protected IT environment.

PRODUCT DESCRIPTION

Desigo CC is the integrated building management platform for managing high-performing buildings. With its open design, it has been developed to create comfortable, safe and efficient facilities. It is easily scalable from simple single-discipline systems to fully integrated buildings.

Desigo CC Compact extends the portfolio with a tailored solution for small and medium-sized buildings.

GMA-Manager allows for functionally combining different safety and security systems such as fire detection systems and video surveillance on a single common platform.

Operation Scheduler is a tool that enables security operators to intelligently perform routine tasks. It can be used to schedule maintenance tasks.

Siveillance Control is a Physical Security Information Management system (PSIM) that seamlessly consolidates a variety of safety and security systems, such as access control, intrusion detection, and video surveillance, all on one common platform.

Siveillance Control Pro is a command and control solution, specifically designed to support security management at critical infrastructure sites such as ports, airports, oil and gas power generation and distribution, chemical and pharma industries, heavy industries and campus environments.

Siveillance Open Interface Services (OIS) is an interface and integration platform for the integration of subsystems into management stations.

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-2021-31891

The affected application incorrectly neutralizes special elements in a specific HTTP GET request which could lead to command injection.

An unauthenticated remote attacker could exploit this vulnerability to execute arbitrary code on the system with root privileges.

CVSS v3.1 Base Score	10.0
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

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 (2021-09-14): Publication Date

TERMS OF USE