SSA-212009: Vulnerabilities in Siveillance VMS

Publication Date: 2019-06-11
Last Update: 2019-06-11
Current Version: V1.0
CVSS v3.0 Base Score: 8.8

SUMMARY

The latest update for the Siveillance VMS line fixes three security vulnerabilities that can cause remote privilege escalation. Siemens has released updates for the affected products and recommends to update affected devices as soon as possible.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Siveillance VMS 2017 R2: All versions < V11.2a	Update to V11.2a https://support.industry.siemens.com/cs/ww/en/ps/24899/dl
Siveillance VMS 2018 R1: All versions < V12.1a	Update to V12.1a https://support.industry.siemens.com/cs/ww/en/ps/24899/dl
Siveillance VMS 2018 R2: All versions < V12.2a	Update to V12.2a https://support.industry.siemens.com/cs/ww/en/ps/24899/dl
Siveillance VMS 2018 R3: All versions < V12.3a	Update to V12.3a https://support.industry.siemens.com/cs/ww/en/ps/24899/dl
Siveillance VMS 2019 R1: All versions < V13.1a	Update to V13.1a https://support.industry.siemens.com/cs/ww/en/ps/24899/dl

WORKAROUNDS AND MITIGATIONS

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

- Block port 80/TCP at an external firewall.

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.

 © Siemens AG 2019

PRODUCT DESCRIPTION

Siveillance VMS is a powerful IP VMS (Video Management Station) platform family scaling from smaller to large complex deployments. The Siveillance VMS portfolio consists of four versions, Siveillance VMS 50, 100, 200 and 300, addressing the specific needs of small and medium size solutions up to large complex deployments.

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-2019-6580

An attacker with network access to port 80/TCP could change device properties without authorization. No user interaction is required to exploit this security vulnerability. Successful exploitation compromises confidentiality, integrity and availability of the targeted 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-2019-6581

An attacker with network access to port 80/TCP could change user roles without proper authorization.

The security vulnerability could be exploited by an authenticated attacker with network access to the affected service. No user interaction is required to exploit this security vulnerability. Successful exploitation compromises confidentiality, integrity and availability of the targeted 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-2019-6582

An attacker with network access to port 80/TCP can change user-defined event properties without proper authorization.

The security vulnerability could be exploited by an authenticated attacker with network access to the affected service. No user interaction is required to exploit this security vulnerability. Successful exploitation compromises integrity of the user-defined event properties and the availability of corresponding functionality.

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:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:L/E:P/RL:O/RC:C

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.