SSA-457058: .NET Security Vulnerability in Siveillance VMS

Publication Date: 2018-05-03
Last Update: 2018-05-23
Current Version: V1.1
CVSS v3.0 Base Score: 8.1

SUMMARY

Siemens has released software updates for Siveillance VMS which fix a security vulnerability with the .NET Remoting deserialization that could allow elevation of privileges and/or causing a Denial-of-Service, if affected ports are exposed.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Siveillance VMS 2016 R1 and prior: All versions < V10.0a	Update to V10.0a Obtain the update via your local Siemens representative
Siveillance VMS 2016 R2: All versions < V10.1a	Update to V10.1a Obtain the update via your local Siemens representative
Siveillance VMS 2016 R3: All versions < V10.2b	Update to V10.2b Obtain the update via your local Siemens representative
Siveillance VMS 2017 R1: All versions < V11.1a	Update to V11.1a Obtain the update via your local Siemens representative
Siveillance VMS 2017 R2: All versions < V11.2a	Update to V11.2a Obtain the update via your local Siemens representative
Siveillance VMS 2018 R1: All versions < V12.1a	Update to V12.1a Obtain the update via your local Siemens representative

WORKAROUNDS AND MITIGATIONS

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

- Restrict network access to port 7474/TCP and port 9993/TCP

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

Siveillance VMS is an IP video management software (VMS) designed for deployments ranging from small to large-scale. Its single management interface enables the efficient administration of the system including multiple cameras and security devices.

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-2018-7891

The Recording Server, Management Server, and Management Client on ports 6473/TCP local connection only, 7474/TCP, 8966/TCP local connection only, and port 9993/TCP use an exploitable .NET Framework Remoting deserialization level.

The security vulnerability could be exploited by an attacker with access to the vulnerable ports and could allow elevation of privileges or causing a Denial-of-Service, compromising confidentiality, integrity and availability of the targeted system.

At the time of advisory publication no public exploitation of this security vulnerability was known. Siemens confirms the security vulnerability and provides mitigations to resolve the security issue.

CVSS v3.0 Base Score	8.1
CVSS Vector	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/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 (2018-05-03): Publication Date
V1.1 (2018-05-23): Updated remediation info

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.