SSA-468514: Improper Certificate Validation Vulnerability in Siveillance VMS Video Mobile App for Android and iOS

Publication Date: 2018-05-03
Last Update: 2018-05-03
Current Version: V1.0
CVSS v3.0 Base Score: 4.8

SUMMARY

The latest update for the Siveillance VMS Video mobile app for Android and iOS fixes a security vulnerability that could allow an attacker in a privileged network position to read data from and write data to the encrypted communication channel between the app and a server. Precondition for this scenario is that an attacker is able to intercept the communication channel between the affected app and a server, and is also able to generate a certificate that results for the validation algorithm in a checksum identical to a trusted certificate.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Siveillance VMS Video for Android: All versions < V12.1a (2018 R1)	Update to V12.1a (2018 R1) https://play.google.com/store/apps/details?id=com.siemens.siveillancevms
Siveillance VMS Video for iOS: All versions < V12.1a (2018 R1)	Update to V12.1a (2018 R1) https://itunes.apple.com/us/app/siveillance-vms-video/id1045047239

WORKAROUNDS AND MITIGATIONS

Siemens has not identified any specific mitigations or workarounds.

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

The Siveillance VMS Video Mobile Apps allow to view video from your Siveillance VMS system on your Smartphone or Tablet.

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-2018-4849

Improper certificate validation could allow an attacker in a privileged network position to read data from and write data to the encrypted communication channel between the app and a server.

The security vulnerability could be exploited by an attacker in a privileged network position which allows intercepting the communication channel between the affected app and a server (such as Man-in-the-Middle). Furthermore, an attacker must be able to generate a certificate that results for the validation algorithm in a checksum identical to a trusted certificate. Successful exploitation requires no user interaction. The vulnerability could allow reading data from and writing data to the encrypted communication channel between the app and a server, impacting the communication's confidentiality and integrity.

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	4.8
CVSS Vector	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Karsten Sohr from TZI Bremen for coordinated disclosure

ADDITIONAL INFORMATION

For further inquiries on 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

TERMS OF USE