SSA-511182: Use of Static TLS Certificate Known Hard Coded Private Keys in Adaptec Maxview Application

Publication Date: 2023-04-11
Last Update: 2023-04-11
Current Version: V1.0
CVSS v3.1 Base Score: 6.2

SUMMARY

The Adaptec Maxview application shipped with affected SIMATIC IPCs contains a hard coded, non-unique certificate to secure HTTPS connections between the browser and the local Maxview configuration application. A local attacker may use this key to decrypt intercepted local traffic between the browser and the application and could perform a man-in-the-middle attack in order to modify data in transit.

Adaptec has released updates for the affected products and recommends to update to the latest versions. Siemens recommends countermeasures for products where updates are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC IPC647D: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC IPC647E: All versions with maxView Storage Manager < 4.09.00.25611 on Windows	Update maxView Storage Manager to 4.09.00.25611 or later version https://storage.microsemi.com/en-us/support/raid/sas_raid/asr-3151-4i/ See further recommendations from section Workarounds and Mitigations
SIMATIC IPC847D: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC IPC847E: All versions with maxView Storage Manager < 4.09.00.25611 on Windows	Update maxView Storage Manager to 4.09.00.25611 or later version https://storage.microsemi.com/en-us/support/raid/sas_raid/asr-3151-4i/ See further recommendations from section Workarounds and Mitigations
SIMATIC IPC1047: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC IPC1047E: All versions with maxView Storage Manager < 4.09.00.25611 on Windows	Update maxView Storage Manager to 4.09.00.25611 or later version https://storage.microsemi.com/en-us/support/raid/sas_raid/asr-3151-4i/ See further 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:

- Update the default self-signed device X.509 certificate with an own trusted certificate

Product-specific remediations or mitigations can be found in the section Affected Products and Solution. Please follow the General Security Recommendations.

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

SIMATIC IPC (Industrial PC) is the hardware platform for PC-based automation from Siemens.

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-2023-23588

The Adaptec Maxview application on affected devices is using a non-unique TLS certificate across installations to protect the communication from the local browser to the local application. A local attacker may use this key to decrypt intercepted local traffic between the browser and the application and could perform a man-in-the-middle attack in order to modify data in transit.

CVSS v3.1 Base Score	6.2
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

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 (2023-04-11): Publication Date

TERMS OF USE