

SSA-760124: Multiple Vulnerabilities in Licensing Software for SICAM 230

Publication Date: 2019-02-12
Last Update: 2019-02-12
Current Version: V1.0
CVSS v3.0 Base Score: 10.0

SUMMARY

Multiple vulnerabilities have been identified in the WibuKey Digital Rights Management (DRM) solution, which affect the SICAM 230 process control system.

Siemens recommends users to apply the updates to WibuKey Digital Rights Management (DRM) provided by WIBU SYSTEMS AG.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SICAM 230: All versions <= V7.20	Apply WibuKey Digital Rights Management (DRM) version 6.50 or higher from WIBU SYSTEMS AG https://www.wibu.com/support/user/downloads-user-software.html

WORKAROUNDS AND MITIGATIONS

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

- CVE-2018-3991 can be mitigated by blocking port 22347/tcp e.g. on an external firewall.

GENERAL SECURITY RECOMMENDATIONS

Siemens strongly recommends applying the provided security updates using the corresponding tooling and documented procedures made available with the product. If supported by the product, an automated means to apply the security updates across multiple product instances may be used. Siemens strongly recommends prior validation of any security update before being applied, and supervision by trained staff of the update process in the target environment.

As a general security measure Siemens strongly recommends to protect network access with appropriate mechanisms (e.g. firewalls, segmentation, VPN). It is advised to configure the environment according to our operational guidelines in order to run the devices in a protected IT environment.

Recommended security guidelines to Secure Substations can be found at:

<https://www.siemens.com/gridsecurity>

PRODUCT DESCRIPTION

SICAM 230 is a scalable process control system for a broad range of applications and can be used from an integrated energy system for utility companies to a monitoring system for smart grid applications.

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-2018-3989

A specially crafted IRP (I/O request packet) can cause the driver to return uninitialized memory, resulting in kernel memory disclosure.

CVSS v3.0 Base Score 4.3
CVSS Vector CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N/E:P/RL:O/RC:C

Vulnerability CVE-2018-3990

A specially crafted IRP (I/O request packet) can cause a buffer overflow, resulting in kernel memory corruption and, potentially, privilege escalation.

CVSS v3.0 Base Score 9.3
CVSS Vector CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C

Vulnerability CVE-2018-3991

A specially crafted TCP packet sent to port 22347/tcp can cause a heap overflow, potentially leading to remote code execution.

CVSS v3.0 Base Score 10.0
CVSS Vector CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/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 (2019-02-12): 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.