isssource.com, 14.07.2020

SIEMENS CLEARS SICAM VULNERABILITIES

JUL 14, 2020 | NEWS

Siemens has an update available to handle multiple vulnerabilities in its SICAM MMU, SICAM T and SICAM SGU, according to a report with CISA.

The vulnerabilities include out-of-bounds read, missing authentication for critical function, missing encryption of sensitive data, use of password hash with insufficient computational effort, cross-site scripting, classic buffer overflow, basic XSS, and authentication bypass by capture-replay.

Successful exploitation of these remotely exploitable vulnerabilities could allow an attacker to affect the availability, read sensitive data, and gain remote code execution on the affected devices.

RELATED STORIES

- Phoenix Contact Solution to Automation Worx Holes
- Rockwell Handles Logix Designer Studio 5000 Flaw
- New Version Fixes Mitsubishi GOT2000 Series
- Grundfos Fixes CIM 500 Holes

The following researchers discovered the vulnerabilities: Luca Simbürger, Luca Hofschuster, Lukas Kahnert, Jakob Lachermeier, Christian Costa, Simon Huber, Lukas Sas Brunschier, Florian Freiberger, Florian Burger, Marie-Louise Oostveen, Magdalena Thomeczek, and Johann Uhrmann from Landshut University of Applied Sciences and Max Hirschberger, Simon Hofmann, and Peter Knauer from Augsburg University of Applied Sciences.

The following Siemens products suffer from the issues:

- SICAM MMU: All versions prior to 2.05
- SICAM SGU: All versions
- SICAM T: All versions prior to 2.18

In one issue, by performing a flooding attack against the web server, an attacker might be able to gain read access to the device's memory, and reveal confidential information.

CVE-2020-10037 is the case number assigned to this vulnerability, which has a CVSS v3 base score of 5.9.

In addition, an attacker with access to the device's web server might be able to execute administrative commands without authentication.

CVE-2020-10038 is the case number assigned to this vulnerability, which has a CVSS v3 base score of 9.8.

Also, an attacker in a privileged network position between a legitimate user and the web server might be able to conduct a man-in-the-middle attack and gain read and write access to the transmitted data.

CVE-2020-10039 is the case number assigned to this vulnerability, which has a CVSS v3 base score of 7.5.

In another issues, an attacker with local access to the device might be able to retrieve passwords in clear text.

CVE-2020-10040 is the case number assigned to this vulnerability, which has a CVSS v3 base score of 6.2.

In addition, a stored cross-site-scripting (XSS) vulnerability is present in different locations of the web application. An attacker might be able to take over a session of a legitimate user.

CVE-2020-10041 is the case number assigned to this vulnerability, which has a CVSS v3 base score of 9.6.

Also, a buffer overflow in various positions of the web application might enable an attacker with access to the web application to execute arbitrary code over the network.

CVE-2020-10042 is the case number assigned to this vulnerability, which has a CVSS v3 base score of 9.8.

In another issue, the web server could allow cross-site scripting (XSS) attacks if unsuspecting users are tricked into accessing a malicious link.

CVE-2020-10043 is the case number assigned to this vulnerability, which has a CVSS v3 base score of 8.8.

In addition, an attacker with access to the network could be able to install specially crafted firmware on the device.

CVE-2020-10044 is the case number assigned to this vulnerability, which has a CVSS v3 base score of 9.8.

Also, an error in the challenge-response procedure could allow an attacker to replay authentication traffic and gain access to protected areas of the web application.

CVE-2020-10045 is the case number assigned to this vulnerability, which has a CVSS v3 base score of 8.3.

The products see use in the chemical, energy, food and agriculture, and water and wastewater systems sectors. They also see action on a global basis.

No known public exploits specifically target these vulnerabilities. However, an attacker with low skill level could leverage the vulnerabilities.

Siemens recommends applying updates, where available:

- SICAM MMU: Update to v2.05
- SICAM SGU: For RTU applications, upgrade the discontinued SICAM SGU devices to SICAM A8000 RTUs.
- SICAM T: Update to v2.18

Siemens found specific workarounds and mitigations that users can apply to reduce the risk:

- The firmware updates to SICAM T and SICAM MMU introduce authentication to the web application and remove some unnecessary functionality. The web authentication functionality reduces the risk of access to the device's web application for executing administrative commands by unauthenticated users.
- Due to hardware constraints, encryption is not possible on the devices. Confidential data such as passwords handled by the devices need to be protected on the network by other means.
- The risk for remote code execution and unauthenticated firmware installation can be mitigated by ensuring encryption and authentication between the user and the device, e.g., by VPN.
- Use a modern and up to date browser.

As a general security measure, Siemens recommends protecting network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends configuring the environment according to the Siemens operational guidelines for Industrial Security and following the recommendations in the product manuals.

For additional information, click on Siemens Security Advisory SSA-305120.