Overview

Schneider Electric was notified and is responding to a vulnerability impacting the SUI Software product.

Vulnerability Overview

The vulnerable ActiveX control, GenVersion.dll, is an optional component of WebHMI (complement of the SUI Software).
The optional SUI - WebHMI Server component role over the internet / intranet communication is to:
- deliver WEB-based graphical views, trends and alarms to remote Web browsers
- receive and treat the remote operator's commands.

Product(s) Affected

This vulnerability affects only the WebHMI component of the SUI Software product:

- SUI V1.1 RC6
- SUI V1.1 RC7

Vulnerability Details

Exploitation of this vulnerability requires a user to:
- first to install the affected ActiveX control (Genversion) and
- secondly to visit a page containing a special crafted JavaScript.

By coding a specially crafted string to call the "SetActiveXGUID" method, it might be possible to overflow a static buffer or to execute external code (any binary code). The code could be executed on the user's machine with respect and limits of the logged user's privileges.

Exploitability

The PC-Client requires Windows and Internet Browser. All necessary Web components are remotely delivered and seamlessly installed. The user needs to know the Server IP address.

To open the SUI - WebHMI application, the user shall write the “XXX.XXX.XXX.XXX/webhmi” IP address via the Internet browser (PC-Client). Then, operator is asked to download and install the required ActiveX controls.

This vulnerability is remotely exploitable.

Existence of Exploit

An exploit targeting this vulnerability is publicly available.

Difficulty

This vulnerability requires moderate skill to exploit. Social engineering techniques are also needed to exploit this vulnerability. An understanding of the SUI application and system architecture (IP address) is needed.

Vulnerability level

CVSS scores are a standard way of ranking vulnerabilities and are provided for reference.

Base CVSS Score: 7.1 (AV: NA/ AC: H/ Au: S/ C: C/ I: C/ A: C)

Vulnerability Impact

If successfully exploited, this vulnerability results in remote arbitrary code execution from any remote location based on the privileges of the user. Based on our environment, sending arbitrary code through the SUI-WebHMI can initiate a denial of service or give the possibility to take control of the application.

Containment

- Limit the use of PCs connected to WebHMI server (only this feature, no other use)
- Maintain an updated antivirus on client PCs

Problem resolution

Schneider Electric has released a new patch for SUI in order to address this vulnerability.

- Install the corrective patch (See patch procedure)

This patch requires a reboot of the host machine (SUI)

For More Information

This document is intended to help provide an overview of the identified vulnerability and actions required to mitigate it. To obtain full details on the issues and assistance on how to protect your installation, please contact your local Schneider Electric representative. These organizations will be fully aware of the situation and can support you through the process.

For further information on vulnerabilities in Schneider Electric's products, please visit Schneider Electric's Cybersecurity web page at http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page

About Schneider Electric

As a global specialist in energy management with operations in more than 100 countries, Schneider Electric offers integrated solutions across multiple market segments, including leadership positions in Utilities & Infrastructures, Industries & Machine Manufacturers, Non-residential Buildings, Data Centers & Networks and in Residential.
www.schneider-electric.com