Overview

Schneider Electric was notified and is responding to a vulnerability in the MiCOM S1 Studio Software product. This software utility is used to configure and maintain electronic protective relays.

Vulnerability Overview

The vulnerability is an issue with the MiCOM S1 Studio installer routine. During install, Read/Write access by any user is permitted to MiCOM S1 Studio executables in the Program Files directory. This condition persists after installation. As a result of this access, the configuration files and the Windows service used by the program can be manipulated or modified by any user with local computer access.

Product(s) Affected

The product affected includes:

- MiCOM S1 Studio Software, up to V3.5.2 version.

Vulnerability Details

- Modification of the Windows service could allow the actor to escalate their privileges on the local computer. This attack is not considered to be remotely exploitable.
- Modification of the protective relay configuration files could cause the user to inadvertently download incorrect parameters to the Intelligent Electronic Device resulting in misoperation. This attack is not considered to be remotely exploitable.

Mitigation

MiCOM S1 Studio software was developed with the expressed intention of providing an easy means for maintenance personnel to modify or manage the configuration parameters of

electronic protective relays. This software is designed to be used in close proximity to the protective relay. It is always a real possibility that configuration parameters being downloaded to an intelligent device like a protective relay can be mistyped or entered in error. Standard practices always encourage users to validate the downloaded parameters through the devices' front panel HMI. Even if configuration files are manipulated by bad actors, this simple check on the front panel will ensure the device's parameters are set to the correct value.

To protect the computer from unauthorized escalation of privileges through manipulation of the Windows service routine installed with the software, Schneider Electric recommends users employ best IT practices to secure their computer with authorized user login and password protection. For Windows 7 configured computers, use of User Access Control (UAC) can further improve the security of the computer. Additionally, to minimize the risk of attack, users who are not directly using this software on a regular basis are strongly encouraged to delete this application from their computer to reduce the likelihood of attack.

Solution available in MiCOM S1 Studio V4.0.1 (August 2013)

The installation routine of MiCOM 1 Studio V4.0.1 provides digital signature to all files related to the use of MiCOM S1 Studio:

- Digital signature indicates to the operating system and the user that the libraries/executables are from Schneider Electric (Trusted source).

Solution available in MiCOM S1 Studio V5.0.0 (April 2014)

The installation routine of MiCOM 1 Studio V5.0.0 provide the following features:

- Compiler option Nx compact settings has been enabled to avoid any security threat.
- Folder privileges have been set as read only (only for folders and files under TARGETDIR)
- Executable privileges have been marked as read only to avoid any escalation of privileges to perform malicious operation.

Link to our web site to download MiCOM S1 Studio V5.0.0:

- http://www.schneider-electric.com/products/ww/en/2300-ied-user-software/2310-micom-user-software/61035-micom-s1-studio/

CONCLUSION

Schneider Electric has worked strongly to finalize and resolve all issues raised in this document.

Schneider Electric recommend to all customers and users to install and use MiCOM S1 Studio V5.0.0.

Acknowledgements

Schneider Electric would like to thank researcher Michael Toecker for all his efforts related to identification of this vulnerability and its disclosure.

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