GE VERNOVA

Grid Automation
Protection Automation Control

Security Notice

Date: **13 January 2025** Distribution: **Public** Reference: **GES-2025-001**

Affected Product Family ‘S1 AGILE’ Software

MiCOM S1 Agile:
Privilege Escalation Vulnerability

References

Publication Number	GES-2025-001
Release Date	13 January 2025

Overview

The S1 Agile Engineering ToolSuite software is for MiCOM P40 relays. S1 Agile supports all existing MiCOM P40 Agile ranges including legacy products.

It has been brought to our attention that any malicious user or attacker can possibly modify or replace a file, which is used by S1 Agile to gain “Administrator” privileges on the workstation. This weakness is corrected in versions 3.1.0 and later.

Please refer to the “Vulnerability details” section for more details.

GE Vernova thanks Charit Misra from DNV, Netherlands for responsibly disclosing the vulnerabilities in our product to our PSIRT team, and their engagement with GE Vernova on such matters.

At the time of issuing this document, there are no reported cybersecurity attacks which have exploited the vulnerability in this document. GE Vernova is addressing this vulnerability as part of its commitment to improve security in our products.

Background

MiCOM S1 Agile is the IED engineering ToolSuite for MiCOM P40 Agile IEDs. All tools are assembled in a palette for simple entry, with intuitive navigation via a few mouse-clicks. MiCOM S1 Agile supports all existing MiCOM P40 Agile ranges including legacy products such as K-series and Modulex and includes a utility for automatic conversion of setting files from previous generations of numerical relays like K-series and MiCOM P20 to the latest P40 Agile models. MiCOM S1 Agile is presented as “tiles” rather than menu items to provide a more intuitive user experience.

Key Features in the MiCOM S1 Agile ToolSuite:

- GE Vernova’s integrated engineering tool that provides users with access to MiCOM P40 Agile IEDs configuration and record data.
- Integrated configuration and monitoring features.
- Send and extract setting files.
- Event and disturbance record extraction and analysis.
- Integrated programmable curve tool, and redundant Ethernet configuration for protection relays.
- Integrated automatic extraction of disturbance records facility.
- Integrated P740 and P746 remote HMI and topology tools for busbar schemes.

The MiCOM P40 Agile family of advanced protection and control relays provides one integrated platform that delivers leading edge protection, control, monitoring, and metering solutions for critical power system applications. The MiCOM P40 Agile platform supports proven protection algorithms, expandable I/O, integrated monitoring, and accurate metering capabilities with the latest in communications technologies. The MiCOM P40 family of devices provides the situational awareness needed for a reliable, secure and efficient modern grid.

MiCOM P40 Agile relays are digital devices designed to be installed and operated in a utility & industrial environment and connected to secure private networks.

Vulnerability Details

GE Vernova received a report regarding this S1 Agile vulnerability from an external researcher. By some means, if an attacker can replace a legitimate exe file with a malicious exe file in one of the S1 Agile application folders, and the computer restarts, then the attacker’s code may get executed. In a worst scenario, the remote attacker may get “administrator” privileges to the computer on which S1 Agile is installed.

The potential attacker must have access to the workstation with basic privileges on the computer to perform this attack.

Affected Products/Versions

MiCOM S1 Agile is the IED engineering ToolSuite for MiCOM P40 Agile relays.

Products	Versions
S1 Agile IED engineering ToolSuite	All firmware versions prior to version 3.1.1

Workaround/Mitigation

As a workaround, GE Vernova recommends having sufficient security controls in place on the workstation where S1 Agile software is installed. This will ensure the attacker's remote connection to the computer is not feasible. Harden the computer on which S1 Agile is installed. The product deployment guide can be used to understand the guidelines around how the product can be deployed in the end user's environment.

Resolution

To resolve this issue and enhance security, during the S1 Agile application installation, we ensure only privileged users can access various folders used by the S1 Agile application. This ensures that S1 Agile files can not be edited or replaced by users without sufficient privileges on that computer.

We would like to assert that this attack, if successful, can give "Administrator" privileges to the attacker on the computer, but the configured IEDs will not see any impact in their configuration or functionality. The RBAC ('Role-Based Access Control') on the IED remains unimpacted.

We strongly recommend customers to upgrade to the latest software version available. Software version 3.1.1 is released for customer usage in January 2025.

Products	Versions
MiCOM S1 Agile	All versions through 3.1.0

GE Product Security Incident Response Team (PSIRT)

GE is committed to helping ensure the security of its customer base. To report product security issues and to request security support, contact PSIRT online at http://www.gevernova.com/security or by email at security@ge.com.

For Product Support

For questions or further product support, please contact the GE Vernova support team using:

Region	E-mail	Telephone
Global Contact Centre	GA.support@gevernova.com	+44 1785 250070
Central, East Asia, Pacific	GA.supportCEAP@GE.com	+61 414 730 964
India	GA.supportIND@GE.com	+91 44 2264 8000
Middle East, North Africa, Turkey	GA.supportMENAT@gevernova.com	+971 42929467
Europe, Russia, CIS, Sub-Saharan Africa	GA.supportERCIS@gevernova.com	+34 94 4858854
North America	GA.supportNAM@gevernova.com	+1 877 605 6777
Latin America	GA.supportLAM@gevernova.com	+55 48 2108 0300

Document Revision History

Version	Date	Change Description
GES-2025-005	13 January 2025	Initial release

Disclaimer

Unless the product is under a GE Vernova service contract, GE Vernova assumes no responsibility or liability for the content of Security Notices or for making Security Notices available to the customer.

Implementing Security Notices as well as performing updates/upgrades to software/firmware is solely the responsibility of the customer.