GE
Grid Solutions

## Reason RPV311

# Flash Player EOL and hard-coded credentials on RPV311

# Security Notice

GE Publication Number: GES-2021-005

Security: GE Proprietary Information – Public

Release Date: 26 March 2021
CVSS: See below in "Vulnerability details"
ICS-CERT Advisory:
CVE Identifier:

## Overview

Zero Day Initiative OT Security Team found a vulnerability in GE Grid Solution Reason RPV311 multifunctional digital fault recorder (DFR) including hard-coded credentials which could allow adversaries to partially take control of the DFR. In parallel Adobe has discontinued Flash Player plugin, causing security concerns. This document provides more information on the nature of these vulnerabilities as well as the recommended mitigation steps for RPV311 with the affected firmware versions.

## Background

RPV311 is a Multifunctional Digital Fault Recorder (DFR). GE's Reason RPV311 has distributed architecture capable to acquire data through IEC 61850-9-2LE sampled value subscription or proprietary protocol interface with remote acquisition units RA331, RA332 or RA333, connected to conventional current and voltage transformers. The RPV311 calculate measures based on acquired data and is capable to generate fault, disturbance, continuous, steady-state and sequence of events records with flexible thresholds and triggers configured by the user. As multifunctional platform, the RPV311 also has capabilities for applications as PMU, power quality and precise fault location using Traveling Waves methods.

The Multifunctional Digital Fault Recorder RPV311 is designed to be installed and operated in industrial and power sub-station environments and connected to private networks.

## Vulnerability details

The next vulnerabilities where found in RPV311:

- Use of hard-coded password in the device. Adversaries could take limited control of the fault recorder using some hard-coded credentials.
    - CVSS: 6.3 (severity **medium**)
    - Note that the impact is limited considering that the device is designed to be connected to private networks, installed and operated in closed/protected industrial and power substation environments, which reduces exploitability.
- Use of Adobe Flash Player Plugin after EOL period (potential vulnerability no CVSS)

Thanks to Zero Day Initiative OT Security Team who initially reported the first vulnerability.

## Affected products/versions

| **Products** | **Versions** |
|---|---|
| RPV311 | All firmware versions prior or equal to v14A03 |

## Workarounds and mitigation

Considering the RPV311 is designed to be installed and operated in industrial and power substation environment, in applications where it is not needed access to public networks, for the vulnerabilities herein described GE recommend RPV311 devices to be protected using network defense-in-depth practices. This includes, but is not limited to, placing RPV311 devices inside the control system network security perimeter, and having access controls, monitoring (such as an Intrusion Detection System), and other mitigating technologies in place.

Regarding Flash player plugin, Adobe has decided the end-of-life for product due to vulnerabilities. To reduce risks of existent vulnerabilities protective mechanisms for blocking access to malicious Flash Player movies were implemented. To overcome these mechanisms in a safe way GE recommends the users to update Flash Player configuration file whitelisting the IP addresses of the desired RPV311 by following the procedure named "*How to use Reason RPV311 webinterface after Flash Player end-of-life*", available at https://www.gegridsolutions.com/products/support/Application-Note-RPV311-FlashPlayer.pdf.

## Product support

For help with any aspect of your GE Grid Solutions product, please contact our support team, 24/7, as follows:

| Region | E-mail | Telephone |
|---|---|---|
| Global Contact Centre | ga.support@GE.com | +44 1785 250070 |
| Central and East Asia and Pacific | ga.supportCEAP@GE.com | +61 414 730 964 |
| India | ga.supportIND@GE.com | +91 44 22648000 |

| | | |
|---|---|---|
| Middle East, North Africa and Turkey | ga.supportMENAT@GE.com | +971 42929467 |
| Europe, Russia, CIS and Sub-Saharan Africa | ga.supportERCIS@GE.com | +34 94 4858854 |
| North America | ga.supportNAM@GE.com | +1 877 605 6777 |
| Latin America | ga.supportLAM@GE.com | +55 11 36187308 |

## 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.ge.com/security or by email at security@ge.com.

## Document revision history

| Version | Date | Change description |
|---|---|---|
| GES-2021-005 | 26 March 2021 | Initial release |
| | | |