Xylem Product Security Advisory

Rockwell ISaGRAF Runtime vulnerabilities for Flygt MultiSmart

June 8, 2021

Overview & Impact

Rockwell Automation recently announced security vulnerabilities which impact ISaGRAF Runtime v5.x, which is a feature that can be enabled in the **Flygt MultiSmart pump station management system**.

These vulnerabilities in Rockwell Automation's software ***do not affect most MultiSmart devices.***

However, MultiSmart Gen-1 devices and MultiSmart Gen-2 devices running firmware prior to version 3.2.0 contain a version of ISaGRAF 5.x. If ISaGRAF is enabled on those device, then they might be affected by these vulnerabilities.

Users may refer to the MultiSmart Technical Product Information to determine their firmware version (see Section 6.2.4 of the Installation, Operations, and Maintenance Manual). That documentation also provides guidance on enabling and disabling the ISaGRAF feature (see Section 6.2.5.40 of the Installation, Operations, and Maintenance Manual).

Certain pump operation architectures with MultiSmart are vulnerable if the ISaGRAF feature is enabled, and could allow unauthorized users to read, download, or delete content from the device. Please refer to the recommendations in the mitigation section below to reduce the risk of these vulnerabilities.

MultiSmart devices are NOT affected by the vulnerabilities if:

- They were purchased in the last 7 years (since 2014).
- They are running firmware versions 3.2.0 or later.
- The ISaGRAF feature has not been enabled. (It is disabled by default.)

Affected Products and Versions

- ISaGRAF Runtime v5.x
- MultiSmart Gen-1 devices
- MultiSmart Gen-2 devices running firmware versions prior to 3.2.0

Mitigation

Upgrade MultiSmart firmware to version 3.2.0 or later. (Recommended for all MultiSmart Gen-2 devices.)

- Please refer to the MultiSmart release notes located on the Technical Product Information site for instructions on how to upgrade the firmware. (See Section 8.1 of the Installation, Operations, and Maintenance Manual.)

When applicable, upgrade the unit to the latest hardware.

- Users of Gen-1 devices should consider upgrading to Gen-2 devices.
- Please consult with Xylem's Flygt Transport Team for assistance with upgrading the hardware.

Xylem also recommends a comprehensive defense-in-depth strategy to reduce the risk of these vulnerabilities. This means employing adequate network segmentation and security controls including, but not limited to:

- Restricting network connections and confirming the devices are not accessible from the Internet.
- Harden workstations that connect to the MultiSmart devices (e.g., maintain Endpoint Detection & Response solutions, application whitelisting, remove administrative rights).
- Ensuring control devices are behind firewalls and isolated from the enterprise/business network or any other wide-area network.
- Continuously monitor affected devices for security events that could warn of attempted unauthorized use.
- Strictly managing remote access and any privileged access to all devices that can connect to the MultiSmart.

References

- Xylem Product Security Advisories
- Rockwell Security Advisory
- CVE-2020-25182, CVE-2020-25176, CVE-2020-25178, CVE-2020-25184, CVE-2020-25180
    - NIST National Vulnerability Database (NVD) and MITRE CVE® List
- ICSA-20-280-01 - CISA ICS-CERT Advisory
- MultiSmart Technical Product Information

Contact Information

For any questions related to this Xylem Product Security Advisory, please contact product.security@xylem.com.

Disclaimer

This document is provided on an as is basis and does not imply any kind of guarantee or warranty, including the warranties of merchantability or fitness for a particular use. Use of the information on the document or materials linked from the document is at your own risk. Xylem reserves the right the change or update this document any time.