IOActive Security Advisory

Title	GE Grid Solutions Reason RT430 GNSS Precision-Time Clock Multiple Vulnerabilities
Severity	9.6 (Critical) – CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:L/I:H/A:H
Discovered by	Ehab Hussein
Advisory Date	May 14, 2020

Affected Products

GE Grid Solutions Reason RT430, RT431, and RT434 GNSS Precision-Time Clocks

Affected Versions: All firmware versions prior to 08A05

Impact

An unauthenticated attacker with access to the device's web application could:

- Run arbitrary system commands on the device as the 'root' user
- Change the password for the 'configuration' user, which administers the device
- Reboot the device
- Cause a persistent denial of service (DoS) to the device
- Bypass the authentication presented by specific areas of the web application

Background

GE Grid Solutions' Reason RT430 GNSS Precision-Time Clock is referenced to GPS and GLONASS satellites. Offering a complete solution, these clocks are the universal precision time synchronization units, with an extensive number of outputs which supports many timing protocols. including the DST rules frequently used on power systems applications. In accordance with IEEE 1588 Precision Time Protocol (PTP), the RT430 is capable of providing multiple IEDs synchronization with better than 100ns time accuracy over Ethernet networks. Despite being likely to never lose time synchronization from satellites, the RT430 GNSS features a TCXO as its standard internal oscillator ensuring free-running accuracy when clock is not locked.[1]

IOActive found that the RT430's web application exposed several shell scripts that allowed authentication to be bypassed, leading to a full compromise of the device.

[1] https://www.gegridsolutions.com/measurement_recording_timesync/catalog/rt430.htm

Technical Details

Unauthenticated Remote Command Execution

The remote web server hosts scripts that fail to adequately sanitize request strings. By leveraging this issue, an attacker may be able to execute arbitrary commands on the remote host.

The RT430's web application exposes an `endpoint that allows` an unauthenticated attacker could exploit access to this endpoint to inject code into a parameter within the `POST` request body in order to execute arbitrary commands on the system with 'root' permissions.

Unauthenticated Device Persistent DoS

An unauthenticated attacker can send a request to a specific URL on the device which causes it to become unresponsive. This is a result of the device not fully checking the IP addresses being set on the device.

Unauthenticated Password Change for Configuration User

The RT430's web application exposes an endpoint that allows an unauthenticated attacker to change the password for the 'configuration' user account. The attacker could then reconfigure the device using the 'configuration' account along with the new credentials created.

Web Authentication is Checked Client-side in Browser

An attacker could bypass authentication in the web application by manipulating areas of the website's Javascript code that are presented in the web browser. The RT430's web application appears to perform some authentication checking on the client side (browser) in some areas of the web application, which is easy to bypass. An attacker could exploit this access to reconfigure the device.

Unauthenticated Remote Device Reboot

The RT430's web application exposes an endpoint that allows an unauthenticated attacker to access to this endpoint to the reboot the system via a `GET` request.

Fixes

Upgrade to the latest firmware version: 08A05

Timeline

2019-12-17: IOActive discovers vulnerabilities

2020-01-15: IOActive reports vulnerabilities to vendor

2020-03-17: Vendor releases new firmware version 08A05 to address the vulnerabilities

2020-03-17: Vendor releases "PRSN-2020-001 Security Advisory: Reason RT Clocks Vulnerabilities"

2020-05-14: IOActive publishes advisory