Triangle Microworks SCADA Data Gateway – Authentication Bypass | CVE-2023-39457

Overview

A vulnerability in Triangle Microworks' SCADA Data Gateway was published on August 4th, 2023 under the ID CVE-2023-39457. It describes the potential for a remote, unauthenticated used to execute arbitrary code as root on the target system.

Severity

The vendor has set the severity of this issue with a CVSSv3 score of 9.8 (Critical).

Affected Products and Versions

GE Gas Power Products with affected firmware:

- Triangle Microworks SCADA Data Gateway v5.0.0 through v5.1.3

GE Gas Power has had no reports of compromise or exploitation of this vulnerability across any of our customer sites.

Vulnerability Details

This vulnerability affects Triangle Microworks SCADA Data Gateway versions 5.0.0 – 5.1.3. Versions 4.x or earlier are not impacted by this vulnerability. Vulnerable versions of SCADA Data Gateway have the potential for a remote attacker to execute arbitrary code on the system as a root user without requiring authentication to the system. As a result, Triangle Microworks has published a new firmware update (v5.2.0) to address this issue and recommends all customers update their systems to this new version.

Remediation/Mitigation

GE Gas Power has completed validation of SCADA Data Gateway v5.2.0 to ensure that installing the update will not impact the intended operation of equipment. All customers using Triangle Microworks SCADA Data Gateway are strongly recommended to install this new version on their equipment.

We recommend allowing the GE Gas Power engineering team to perform this update on your behalf. Please reach out to your local GE Services representative for support.

Contact Information

Contact your local GE Services representative for assistance or for additional information.
For Product Security issues or incident/vulnerability reporting: www.ge.com/power/cybersecurity

Document History

Version	Release Date	Purpose
1.0	12/21/2023	Initial Release