Vulnerability In Baker Hughes Bently Nevada 3500 | CVE-2021-32997

Overview

GE Gas Power became aware of a vulnerability affecting Baker Hughes Bently Nevada. Successful exploitation of these vulnerabilities could allow an attacker to access to system credentials.

Affected Product and Version

The vulnerability impacts the following software versions of Bently Nevada 3500:

- System 1 6.x, Part No. 3060/00, Versions 6.98 and prior, Released Dec 2020
- System 1, Part No. 3071/xx & 3072/xx, Versions 21.1 HF1 and prior, Released July 2021
- 3500 Rack Configuration, Part No. 129133-01, Versions 6.4 and prior, Released May 2020
- 3500/22M Firmware, Part No. 288055-01, Versions 5.05 and prior, Released May 2021

Vulnerability Details

Use of Password Hash With Insufficient Computational Effort (CWE-916)

The affected products utilize a weak encryption algorithm for storage and transmission of sensitive data, which may allow an attacker to more easily obtain credentials used for access.

Exploitation Status

GE Gas Power Product Security is not aware of any malicious attempts to exploit this vulnerability.

Mitigations

To address this vulnerability, Bently Nevada recommends users obtain 3500 Rack Configuration Version 6.6 or higher from Bently Nevada, which now includes a feature to set enhanced password security. For users that have their 3500 System(s) connected to Bently Nevada's System 1 software, enhanced password security is supported for System 1 Version 21.2 and higher. Using enhanced password security on the 3500 system will break communications with any earlier version of System 1 below Version 21.2

If users are unable to install the latest version of 3500, Bently Nevada recommends implementing the following temporary mitigations:

- Use a unique password for each device.
- Only install affected devices on a secured network.
- Bently Nevada product users with a valid Maintenance & Support Agreement may submit questions to Bently Nevada

Additional Recommendations

GE Gas Power Cybersecurity and Engineering teams will continue to investigate internally as well as monitor industry-based news for any changes or updates. To reduce the risk that vulnerabilities like this may represent to the controls network, we recommend the implementation of a good defense-in-depth strategy as detailed in our GEH 6839 Secure Deployment Guide. Some of our recommended controls include:

- Minimize network exposure for all Controllers with the use of network segmentation, placement of controllers behind controls network firewalls and ensure that they are not accessible from the Internet.
- Block suspicious external IP addresses at the controls network firewalls. Monitor traffic internally for unusual behavior.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize VPN is only as secure as its connected devices.
- Implement defense-in-depth within the controls network environment consisting of tools such as Intrusion Detection/Prevention Systems (IDS/IPS), firewalls, and network access control (NAC).
- Implement and maintain an anti-malware solution and an endpoint detection and response (EDR) solution.
- Disable remote access services and protocols such as Remote Desktop Protocol (RDP) unless needed. Monitor and restrict remote access usage on a least-privilege basis.
- Have backup and restore processes and procedures in place for disaster recovery and incident response.
- Monitor and maintain account provisioning and access control based on the principle of least privilege.

GE Power Product Security Incident Response Team (PSIRT)

Providing secure and reliable products and solutions is vital to the operations of GE Gas Power. Our products are engineered with security as a key principle. We have implemented and will maintain reasonable and appropriate technical and organizational measures, internal controls, and information security routines intended to help protect our products and customers.

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	March 13th, 2022	Initial release
2.0	September 29th, 2022	Updated document classification details