Vulnerability in QNX Neutrino Kernel|CVE-2021-32025

Summary

Based on what has been publicly released to this point, and the information from the GE Gas Power Intel team, the vulnerability does not target any GE products specifically. GE currently evaluates this as a lower overall risk to GE Gas Power customers.

BlackBerry recently published an elevation of privilege vulnerability in the QNX Neutrino Kernel of affected versions of QNX Software Development Platform (SDP), QNX OS for Medical (QOSM), and QNX OS for Safety (QOS) that could potentially allow a successful attacker to access data, modify behavior, or permanently crash the system. To exploit this vulnerability, an attacker must either persuade a user to execute malicious code or exploit an unrelated weakness to gain unrestricted ability to execute code

Impact

The successful exploitation of this vulnerability may enable actors to potentially access data, modify behavior, or permanently crash the system.

Vulnerable

From the BlackBerry Security Advisory of January 11, 2022, the affected QNX products and versions include

- QNX SDP 6.4.0 to 7.0
- QNX Momentics all 6.3.x versions
- QNX OS for Safety versions 1.0.0 to 1.0.2 safety products compliant with IEC 61508 and/or ISO 26262
- QNX OS for Safety 2.0.0 to 2.0.1 safety products compliant with IEC 61508 and /and or ISO 26262
- QNX OS for Medical versions 1.0.0 to 1.0.1 safety products compliant with IEC 62304
- QNX OS for Medical versions 2.0.0 safety products compliant with IEC 62304

Recommendation

To minimize the risk of vulnerabilities such as the QNY Neutrino Kernel vulnerability, 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.
- Running the Mark VIe controller(s) in Secure Mode
- 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 designed 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

Additional Resource(s)

- BlackBerry: QNX-2021-001 Vulnerability in QNX Neutrino Kernel Impact Software Development Software Platform (SDP), QNX OS for Medical, and QNX OS for Safety

Document History

Version	Release Date	Purpose
1.0	February 14th, 2022	QNX Neutrino Kernel Vulnerability Assessment and Potential Product Impact Statement
2.0	February 23rd, 2022	Revised Contact Information
3.0	February 24th, 2022	Revised Contact Information