GE Vernova Security Advisory

Blackberry QNX – Vulnerabilities in OpenSSL, Libexpat, Libxml

Overview

A set of vulnerabilities impacting Blackberry's QNX platform were disclosed by Blackberry on July 18, 2024. These vulnerabilities can potentially lead to remote code execution, information disclosure, or denial of service impacting the OpenSSL, OpenSSH, io-pkt, Libexpat, and Libxml libraries.

Affected Products and Versions

QNX SDP 7.1

Vulnerability Details

ISSUE	BASE SCORE	ADJUSTED SCORE	LIBRARY	DESCRIPTION
CVE-2022-1292	9.8 (Critical)	8.1 (High)	OpenSSL	OS Command Injection (CWE-78)
CVE-2024-6119	7.5 (High)	2.5 (Low)	OpenSSL	Access of Resource Using Incompatible Type (CWE-843)
CVE-2024-6387	8.1 (High)	6.1 (Medium)	OpenSSH	Signal Handler Race Condition (CWE-364)
CVE-2024-35215	6.2 (Medium)	5.1 (Medium)	Io-pkt	Null Pointer Dereference (CWE-476)
CVE-2024-28757	7.5 (High)	6.5 (Medium)	Libexpat	XML Entity Expansion Attack
CVE-2024-25062	7.5 (High)	6.5 (Medium)	Libxml	Use After Free (CWE-416)

Note: Adjusted Score is an environmental score calculated according to impact with regards to compensating controls and overall system impact in the customer environment.

For Gas Power customers, these vulnerabilities impact the UCSE, UCSC, and UCSB controller utilized in the Mark* VIe Platform.

Exploitation Status

GE Vernova has not yet observed nor received reports of any Gas Power customer equipment being compromised by these vulnerabilities.

Remediation/Mitigation

GE Vernova has completed validation for these updated libraries and has released the following updates to ControlST addressing these issues:

ControlST 8.00.08C SP01
ControlST 7.10.02C SP09

GE Vernova recommends that customers running ControlST 7.10 or 8.0 update their installation to the corresponding branch listed above. The issues described above do not impact ControlST 7.9 and earlier versions, as these distributions utilize an earlier version of QNX that does not include these vulnerable library versions.

GE Vernova reserves the right to vary its findings and conclusions should any information or technical knowledge come to GE after the date of this document. This Security Advisory does not vary any contractual relationship between GE Vernova and its customer. NO REPRESENTATION OR WARRANTY IS MADE OR IMPLIED AS TO ITS COMPLETENESS, ACCURACY, OR FITNESS FOR ANY PARTICULAR PURPOSE.

Contact Information

Contact your local GE Vernova Services representative for assistance or additional information.
For Product Security issues or to report an incident/vulnerability, visit
https://www.gevernova.com/security

Document History

Version	Release Date	Purpose
1.0	12/4/2024	Initial Release

Disclaimer

Unless the product is under a GE Vernova service contract, GE Vernova assumes no responsibility or liability for the content of Security Notices or for making Security Notices available to customer. Implementing Security Notices as well as performing updates/upgrades to software/firmware is solely the responsibility of the customer.