Cylon

29 August 2019

Technical Bulletin | Update INTEGRA™ Software: QNX Vulnerabilities

Cylon Technical Bulletin
CVSS v3.0 Base Score: 4.4 (AV:L/AC:L/PR:H/UI:N/S:U/C:H/i:N/A:N)
Defect# HAREMB-1220
CVSS v3.0 Base Score: 8.0 (AV:L/AC:H/PR:H/UI:N/S:C/C:H/i:H/A:H)
Defect# HAREMB-1221

Summary

Two vulnerabilities have been discovered in the QNX operating system images distributed by Cylon.

The first is related to a vulnerability that could allow a less-privileged process to gain read access to privileged files.

The second is related to a vulnerability in the QNX procfs service that could allow a less privileged process to gain access to a chosen process's address space.

The following supported platforms are impacted:

- INTEGRA™ AX 3.8u4 (**IT-8000**)
- INTEGRA™ 4.4u3 (**IT-8000**)
- INTEGRA™ 4.7u1 (**IT-8000**)

Note: INTEGRA™ Windows and Linux Supervisor installations are not impacted.

Cylon has updated the QNX OS images to remove the vulnerability and recommend that users update to the versions identified below:

Cylon Auto-Matrix | Americas
contactus@cylon.com
cylon-automatrix.com

Recommended Action

Cylon has released new updates that mitigate these vulnerabilities.

Product	QNX Patches
INTEGRA AX 3.8u4	OS Dist: 2.7.402.2 NRE Config Dist: 3.8.401.1
INTEGRA 4.4u3	OS Dist: 4.4.73.38.1 NRE Config Dist: 4.4.94.14.1
INTEGRA 4.7u1	OS Dist: (INTEGRA™ IT- 8000) 4.7.109.16.1 NRE Config Dist: 4.7.110.32.1

It is important that all Cylon customers using INTEGRA™ supported platforms update their systems with these releases to mitigate risk. If you have any questions, please contact your Sales Manager or contact Customer Support.

Mitigation

In addition to updating your system, Cylon recommends that customers with affected products take the following protective steps:

- Review and validate the list of users who are authorized and who can authenticate to INTEGRA™.
- Allow only trained and trusted persons to have physical access to the system, including devices that have a connection to the system through the Ethernet port.
- If remote connections to the network are required, consider using a VPN or other means to ensure secure remote connections into the network where the system is located.

Cybersecurity is a priority at Cylon. We are dedicated to continuously improving the security of our products, and we will continue to update you as we release new security features, enhancements, and updates.

Appendix: About CVSS

The Common Vulnerability Scoring System (CVSS) is an open standard for communicating the characteristics and severity of software vulnerabilities. The *Base* score represents the intrinsic qualities of a vulnerability. The *Temporal* score reflects the characteristics of a vulnerability that change over time. The *Environmental* Score is an additional score that can be used by CVSS but is not supplied as it will differ for each customer. The *Base* score has a value ranging from 0 to 10.

Cylon Auto-Matrix | Americas
contactus@cylon.com
cylon-automatrix.com

The *Temporal* score has the same range and is a modification of the *Base* score due to current temporary factors. The severity of the score can be summarized as follows:

Severity Rating	CVSS Score
None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 -8.9
Critical	9.0 - 10.0

A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score.

Detailed information about CVSS can be found on the Forum of Incident Response and Security Team (FIRST) website.

DISCLAIMERS

- Customers and users are responsible for assessing the impact of any actual or potential security vulnerability.
- Your use of the information in this document or materials linked from this document is at your own risk.
- Cylon reserves the right to change or update this document at any time and without notice.
- Cylon provides the CVSS scores 'as is' without warranty of any kind. Cylon disclaims the implied warranties of merchantability and fitness for a purpose and makes no express warranties except as may be stated in a written agreement with and for its customers.
- In no event will Cylon be liable to anyone for any direct, indirect. Special, or consequential damages.

If you have questions regarding this Technical Bulletin, please contact Technical Support. To download a copy of this Bulletin and INTEGRA™ Patch Document login to Toolbox and follow: Technical Bulletins - INTEGRA Patches for HAREMB-1220 and HAREMB-1221.

Product Marketing Team

Cylon Auto-Matrix | Americas
contactus@cylon.com
cylon-automatrix.com