Product Security Bulletin

Important Information - Please Read and Keep

Subject: “NUCLEUS:13” Security Vulnerability

Date: 2021-11-15 (last update)
Originator: Thomas Wood

Background

Security researchers at Forescout Research Labs have discovered new vulnerabilities in the Nucleus TCP/IP network stack (link). The Nucleus network stack is part of the Nucleus real-time operating systems (RTOS) commonly used in medical, industrial and automotive systems. These 13 new vulnerabilities are collectively known as NUCLEUS:13.

What NUCLEUS:13 does

The potential impact of the 13 vulnerabilities identified in NUCLEUS:13 can pose significant risk to devices utilizing the vulnerable TCP/IP network stack. These risks include remote code execution (RCE), information leakage, and denial of service (DoS). The risk scenarios include:

- Buffer overflows in the FTP server due to not validating the length checking in the “USER” command. This can lead to remote code execution.
- A non-null terminated hostname can cause a denial of service and/or read and write out of bounds locations due to the DHCP client lacking input validation.
- Stack-based buffer overflows due to the FTP server not validating the length of the “PWD/XPWD” and “MKD/XMKD” commands. This can cause denial of service and/or remote code execution.
- Information leakage and denial of service conditions due to unchecked lengths of payloads in IP headers for ICMP, TCP and UDP packets.
- Information leakage due to the TFTP server accepting malformed packets that allow for reading the contents of the TFTP memory buffer.
- Denial of service and information leakage caused by corrupted SACK option in TCP packets.
- Denial of service due to the DHCP client not validating the length of Vendor options when processing a DHCP OFFER and OFFER messages.
- Denial of service due to the DHCP client not validating the length of the DNS IP option when processing DHCP ACK messages.
- Potential privilege escalation due to the inability for the client to recognize fake IP options in ICMP echo packets.

Response

Affected Vyaire Products

Vyaire’s products **do not make use** of the Nucleus TCP/IP embedded network stacks or the Nucleus RTOS.

Therefore, **no medical devices** manufactured by Vyaire are directly impacted by these identified vulnerabilities.

How Vyaire Is Responding

Vyaire is monitoring the ongoing situation around the recent disclosures affecting multiple different embedded TCP/IP network stacks.

Vyaire will evaluate information as it becomes available to determine whether any of Vyaire’s products are impacted by the disclosed vulnerabilities

Generic controls

- Ensure your data has been backed up and stored according to your individual process and that your disaster recovery procedures are in place.
- Update your anti-virus and malware protection, where available.

For product or site-specific concerns, contact your Vyaire service representative.

For more information on Vyaire’s proactive approach to product security and vulnerability management, contact us at productsecurity@vyaire.com or visit www.vyaire.com/product-security.

Thomas Wood
thomas.wood@vyaire.com
Product Security Engineer
Vyaire Medical