Product Security Bulletin

IMPORTANT INFORMATION – PLEASE READ AND KEEP

URGENT/11, AMNESIA:33, and NUMBER: JACK Security Vulnerabilities

Date: 2021-03-04 (last update)

Background

Security researchers have found multiple sets of different zero-day vulnerabilities in different embedded TCP/IP network stacks used by a variety of different devices, affecting a range of products from different industries, among those also medical devices:

- Security researchers at Armis have found 11 zero-day vulnerabilities in the network stack developed by VxWorks (summary). The vulnerabilities known as **URGENT/11** affect all devices that support the VxWorks embedded network stack.

- Security researchers at Forescout have found 33 zero-day vulnerabilities in embedded TCP/IP networking stacks (summary). The vulnerabilities known as **AMNESIA:33** affect devices with uIP-Contiki-OS, uIP-Contiki-NG, uIP, open-iscsi, picoTCP-NG, picoTCP, FNET, or Nut/Net embedded network stacks.

- Security researchers at Forescout have found 9 vulnerabilities that affect the TCP/IP stacks (summary) of networked devices. The vulnerabilities known as **NUMBER:JACK** affect devices with uIP, FNET, picoTCP, Nut/Net, cycloneTCP, uC/TCP-IP, MPLAB Net, TI-NDKTCPIP, and Nucleus NET embedded network stacks.

What URGENT/11 Does

The potential impact of the vulnerabilities identified in URGENT/11 can pose significant risk to networked devices supporting the different versions of the VxWorks network stack. The risk scenarios include:

- An attacker from within the network can cause a stack overflow that leads to remote code execution (RCE) by sending specially crafted broadcast or multicast packets.
- An attacker from within or outside the network can trigger a buffer overflow on existing or new connections by manipulating the URGENT flag in the TCP options. This can lead to RCE.

- An attacker within the network can respond to a victim device's DHCP request and cause a heap overflow. This can lead to RCE.
- An attacker within the network can create specially crafted TCP packets with malformed options to trigger a TCP connection to drop causing a Denial of Service (DoS).
- An attacker within the same network can corrupt a victim device's routing table by sending reverse ARP replies to the victim device. This can lead to DoS on the victim device.
- An attacker within the same network masquerading as a DHCP server can send false IPv4 address leading to logical errors on the victim device.
- An attacker within the same network masquerading as a DHCP server can assign the victim device a multicast address, and then sends an IGMPv3 membership query, which causes a DoS on the victim device.
- An attacker within the same network masquerading as a DHCP server can assign the victim device a multicast address, and then sends an IGMPv3 membership query fragmented across several packets leading to the victim device to leak information.

What AMNESIA:33 Does

The potential of the vulnerabilities identified in AMNESIA:33 can lead to DoS, RCE, and information leakage on devices that support the identified embedded network stacks listed above and devices within the network of those vulnerable devices. The risk scenarios include:

- An attacker within the same network sends crafted IPv6 packets to a victim device causing a DoS and information leakage due to errors in header parsing and checking.
- An attacker within the same network can send crafted RPL packets to a victim device with IPv6 enabled causing DoS.
- An attacker within the same network can send crafted TCP/UDP packets to a victim device causing DoS and information leakage due to a flaw in the checksum calculation.
- An attacker within the same network can send crafted TCP packets to a victim device to cause a DoS and information leakage due to TCP option parsing and TCP packet processing errors.
- An attacker within the same network can send crafted fragmented IPv4 or fragmented IPv6 packets to a victim device causing a DoS.
- An attacker within the same network can send DNS replies and poison the DNS cache of the victim device.
- An attacker within the same network can send crafted DNS packets to a victim device causing RCE, DoS, and information leakage due to flawed DNS domain name decoding and DNS response processing.
- An attacker within the same network can send crafted IPv6 DNS packets to a victim device causing RCE due to flawed DNS response parsing in NAT64.

- An attacker within the same network can send crafted ICMPv6 packets to a victim device causing RCE and DoS due to flawed ICMPv6 echo/reply processing.

What NUMBER:JACK Does

NUMBER:JACK is a set of vulnerabilities all related to the initial sequence number (ISN) of a TCP connection. ISNs should be randomly generated, and the network stacks listed above have vulnerabilities that lead to attackers being able to find out the ISNs of TCP connections. The risk scenarios are as follows:

- An attacker from within the network can determine the ISN number on an existing TCP connection and close the connection on the victim device.
- An attacker from within the network can determine the future ISN number on a TCP connection and masquerade as a non-malicious actor.
- An attacker from within the network can determine the ISN number on an existing TCP connection and hijack the TCP session that can lead to data leakage and DoS.

Response

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.

Affected Products

Vyaire's medical devices **do not make use** of the vulnerable TCP/IP embedded network stacks that are affected by URGENT/11, AMNESIA:33, or NUMBER:JACK.

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

Product Security Bulletin

IMPORTANT INFORMATION – PLEASE READ AND KEEP

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.
- Segregate your vulnerable devices on your network to avoid attackers using those devices to attack your other networked devices.
- Patch and update devices to ensure protection from new vulnerabilities.

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

Timo Kosig
timo.kosig@vyaire.com
Product Security Leader
Vyaire Medical

GLOBAL HEADQUARTERS

Vyaire Medical, Inc.
26125 North Riverwoods Blvd
Mettawa, IL 60045
USA

Vyaire Medical GmbH
Leibnizstrasse 7
97204 Hoechberg
Germany

AUSTRALIAN SPONSOR

Vyaire Medical Pty Ltd
Suite 5.03, Building C
11 Talavera Road
Macquarie Park, NSW, 2113
Australia

CE 0123