

UR Family

Wind River TCP/IP Stack (IPnet) Vulnerabilities

Security Notice

Publication Number: GET-20067A

Copyright © 2026 GE Vernova

Security: GE Vernova Public Information – Class I

Initial Release: 30 June 2020

ID: PRSN-2020-002

ICS-CERT Advisory:

ICSA-19-211-01

Updated: 13 July 2020

CVSS: CVSS v3 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) CVE Identifier: CVE-2019-12255,

CVE-2019-12258, CVE-2019-12259, CVE-2019-12261,

CVE-2019-12262, CVE-2019-12263, CVE-2019-12265

Overview

The Universal Relay (UR) Family of products utilizes the WindRiver VxWorks operating system. WindRiver provided notice of 11 TCP/IP network stack vulnerabilities, released by ICS-CERT advisory ICSA-19-211-01.

This document provides more information on applicable vulnerabilities, the nature of the vulnerabilities as well as the recommended action by UR Family users with the affected firmware versions.

Background

The UR Family of advanced protection and control relays provides one integrated platform that delivers leading edge protection, control, monitoring, and metering solutions for critical power system applications. The UR platform supports proven protection algorithms, expandable I/O, integrated monitoring, and high-accuracy metering capabilities with the latest in communications technologies. UR devices provide the situational awareness needed for a reliable, secure, efficient, and modern grid. The intelligent electronic device (IED) is capable of communicating over various protocols, including IEC 61850, DNP3.0, IEC 60870-5-104/103, Modbus, EGD, HTTP, and IEEE 1588.

Vulnerability details

On 30 July 2019, ICS-CERT released security advisory ICSA-19-211-01 regarding certain versions of VxWorks operating system. The UR Family of products is impacted by the following listed vulnerabilities out of 11 reported.

CVE identifier	CVSS	Title	Notes
CVE-2019-12255	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	TCP Urgent Pointer = 0 leads to integer underflow	Access vector: Network (that is, attacker can be anywhere on the Internet and exploit). It can be mitigated with specific rule in firewall. It can be fixed with firmware upgrade.
CVE-2019-12261	AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	TCP Urgent Pointer state confusion during connect () to a remote host	
CVE-2019-12263	AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H	TCP Urgent Pointer state confusion due to race condition	
CVE-2019-12258	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	DoS of TCP connection via malformed TCP options	Access vector: Network. Need firmware upgrade to fix this vulnerability.
CVE-2019-12259	AV:A/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:H	DoS via NULL dereference in IGMP parsing	Access vector: adjacent network access (that is, attacker must be in same local area network as the affected device). Generic cyber security best practices can be used to avoid the attack. Need firmware upgrade to fix these vulnerabilities.
CVE-2019-12262	AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H	Handling of unsolicited Reverse ARP replies (Logical Flaw)	
CVE-2019-12265	AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L	IGMP Information leak via IGMPv3 specific membership report	

See <https://ics-cert.us-cert.gov/advisories/ICSA-19-211-01> for further information about this vulnerability.

Affected products/versions

Products	Versions
UR Family (B30, B90, C30, C60, C70, D30, D60, F35, F60, G30, G60, L30, L60, L90, M60, N60, T35, T60)	Firmware versions 7.0x to 7.91

Workarounds and mitigation

GE Vernova strongly recommends that users with impacted firmware versions update their UR devices to UR firmware version 8.0x, released in June 2020, or greater, to resolve this vulnerability. GE Vernova will work with customers on minor releases with VxWorks patches for affected UR firmware (firmware 7.0x to 7.91).

Out of seven vulnerabilities, four are potentially exploitable remotely and three of the seven vulnerabilities can be mitigated with specific firewall configuration, indicated in the previous table. Details of the firewall mitigation as suggested by Wind River can be found in the [Wind River Security Advisory](#).

GE Vernova recommends that users evaluate their current risk and implement appropriate network security mitigation measures as follows:

- Wind River suggested specific external firewall configuration – Administrators can add a rule to drop/block any TCP-segment where the URG-flag is set
- Effectively segment networks and implement demilitarized zones (DMZs) with properly configured firewalls to selectively control and monitor traffic passed between zones
- Minimize network exposure for all control system devices and/or systems, and ensure that they are not

accessible from the Internet

- Locate control system networks and remote devices behind firewalls, and isolate them from the business network
- Analyze security events to detect early any unexpected traffic/communication

Implementing the mitigation measures listed helps reduce the risk of exploitation until an impacted UR device is updated with firmware containing the Wind River fixes. Note that these mitigation measures do not ensure complete security.

Product support

For help with any aspect of your GE Vernova product, visit our website to contact our support team, 24/7, as follows: <https://www.gevernova.com/grid-solutions/form/grid-technical-support-form>

GE Vernova Product Security Incident Response Team (PSIRT)

GE Vernova is committed to helping ensure the security of its customer base. To report product security issues and to request security support, contact PSIRT online at <http://www.gevernova.com/security> or by email at GEV.PSIRT@gevernova.com.

Document revision history

Number	Date	Change description
GET-20067	30 June 2020	Initial release
GET-20067A	13 July 2020	Changed template and edited document