Security Bulletin CVE-2019-1255-1265

Abstract: Response for ICS-CERT Security Notice

This document will help explain the necessary steps to resolve security issues discussed in the recent announcements regarding the Wind River VxWorks operating system.

Products: Red Lion NT24k Switch Series

Versions Affected: 1.0 through 2.1.10

Revision Information: 2.2.3 Released November 2019

CVE Report	Description	Base Score	Vector	Versions Affected	Remediation
CVE-2019-12255	Wind River VxWorks has a Buffer Overflow in the TCP component (issue 1 of 4). This is a IPNET security vulnerability: TCP Urgent Pointer = 0 that leads to an integer underflow.	9.8 CRITICAL	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	NT24k Switch Series All Firmware Versions from 1.0 to 2.1.10	NT24k 2.2.3 firmwareUpgrade recommended Wind River VxWorks OS patches applied.
CVE-2019-12257	Wind River VxWorks 6.6 through 6.9 has a Buffer Overflow in the DHCP client component. There is an IPNET security vulnerability: Heap overflow in DHCP Offer/ACK parsing inside ipdhcpc.	8.8 HIGH	CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	NT24k Switch Series All Firmware Versions from 1.0 to 2.1.10	NT24k 2.2.3 firmwareUpgrade recommended Wind River VxWorks OS patches applied.
CVE-2019-12260	Wind River VxWorks 6.9 and vx7 has a Buffer Overflow in the TCP component (issue 2 of 4). This is an IPNET security vulnerability: TCP Urgent Pointer state confusion caused by a malformed TCP AO option.	9.8 CRITICAL	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	NT24k Switch Series All Firmware Versions from 1.0 to 2.1.10	NT24k 2.2.3 firmwareUpgrade recommended Wind River VxWorks OS patches applied.
CVE-2019-12258	Wind River VxWorks 6.6 through vx7 has Session Fixation in the TCP component. This is a IPNET security vulnerability: DoS of TCP connection via malformed TCP options.	7.5 HIGH	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	NT24k Switch Series All Firmware Versions from 1.0 to 2.1.10	NT24k 2.2.3 firmwareUpgrade recommended Wind River VxWorks OS patches applied.

REV 1, November 18, 2019

CVE Report	Description	Base Score	Vector	Versions Affected	Remediation
CVE-2019-12261	Wind River VxWorks 6.7 though 6.9 and vx7 has a Buffer Overflow in the TCP component (issue 3 of 4). This is an IPNET security vulnerability: TCP Urgent Pointer state confusion during connect() to a remote host.	9.8 CRITICAL	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	NT24k Switch Series All Firmware Versions from 1.0 to 2.1.10	NT24k 2.2.3 firmware Upgrade recommended Wind River VxWorks OS patches applied.
CVE-2019-12262	Wind River VxWorks 6.6, 6.7, 6.8, 6.9 and 7 has Incorrect Access Control in the RARP client component. IPNET security vulnerability: Handling of unsolicited Reverse ARP replies (Logical Flaw).	9.8 CRITICAL	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	NT24k Switch Series All Firmware Versions from 1.0 to 2.1.10	NT24k 2.2.3 firmware Upgrade recommended Wind River VxWorks OS patches applied.
CVE-2019-12263	Wind River VxWorks 6.9.4 and vx7 has a Buffer Overflow in the TCP component (issue 4 of 4). There is an IPNET security vulnerability: TCP Urgent Pointer state confusion due to race condition.	8.1 HIGH	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H	NT24k Switch Series All Firmware Versions from 1.0 to 2.1.10	NT24k 2.2.3 firmware Upgrade recommended Wind River VxWorks OS patches applied.
CVE-2019-12264	Wind River VxWorks 6.6, 6.7, 6.8, 6.9.3, 6.9.4, and Vx7 has Incorrect Access Control in IPv4 assignment by the ipdhcpc DHCP client component.	7.1 HIGH	CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H	NT24k Switch Series All Firmware Versions from 1.0 to 2.1.10	NT24k 2.2.3 firmware Upgrade recommended Wind River VxWorks OS patches applied.
CVE-2019-12256	Wind River VxWorks 6.9 and vx7 has a Buffer Overflow in the IPv4 component. There is an IPNET security vulnerability: Stack overflow in the parsing of IPv4 packets? IP options.	9.8 CRITICAL	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	The NT24k does not use the vulnerable code in any firmware versions	No action required
CVE-2019-12259	Wind River VxWorks 6.6, 6.7, 6.8, 6.9 and vx7 has an array index error in the IGMPv3 client component. There is an IPNET security vulnerability: DoS via NULL dereference in IGMP parsing.	7.5 HIGH	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	The NT24k does not use the vulnerable code in any firmware versions	No action required
CVE-2019-12265	Wind River VxWorks 6.5, 6.6, 6.7, 6.8, 6.9.3 and 6.9.4 has a Memory Leak in the IGMPv3 client component. There is an IPNET security vulnerability: IGMP Information leak via IGMPv3 specific membership report.	5.3 MEDIUM	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N	The NT24k does not use the vulnerable code in any firmware versions	No action required