# Product Support Notice



PSN # PSN020425u



Original publication date: 08/19/2019 This is Issue #02, published date: 10/29/2019

Severity/risk level Medium Urgency Immediately

Name of problem **PSN020425u – G4xx Gateway WindRiver VxWorks IPNet Vulnerabilities**

## Products affected

G450 Media Gateway

G430 Media Gateway

## Problem description

On the 29th of July 2019, Wind River and security researchers at Armis disclosed a series of vulnerabilities affecting the VxWorks operating system version 6.5 and later.

| CVE | CVSSv3 Score | Title |
|---|---|---|
| CVE-2019-12256 | 9.8 | Stack overflow in the parsing of IPv4 packets' IP options |
| CVE-2019-12257 | 8.8 | Heap overflow in DHCP Offer/ACK parsing inside ipdhcpc |
| CVE-2019-12255 | 9.8 | TCP Urgent Pointer = 0 leads to integer underflow |
| CVE-2019-12260 | 9.8 | TCP Urgent Pointer state confusion caused by malformed TCP AO option |
| CVE-2019-12261 | 8.8 | TCP Urgent Pointer state confusion during connect() to a remote host |
| CVE-2019-12263 | 8.1 | TCP Urgent Pointer state confusion due to race condition |
| CVE-2019-12258 | 7.5 | DoS of TCP connection via malformed TCP options |
| CVE-2019-12259 | 6.3 | DoS via NULL dereference in IGMP parsing |
| CVE-2019-12262 | 7.1 | Handling of unsolicited Reverse ARP replies (Logical Flaw) |
| CVE-2019-12264 | 7.1 | Logical flaw in IPv4 assignment by the ipdhcpc DHCP client |
| CVE-2019-12265 | 5.4 | IGMP Information leak via IGMPv3 specific membership report |

For more information see: https://www.windriver.com/security/announcements/tcp-ip-network-stack-ipnet-urgent11/

The G450 and G430 Media Gateways versions 31.17.0 and later use an affected operating system version. Successful exploitation of those vulnerabilities may have an impact on operation and could allow an unauthorized user to trigger denial of service conditions or execute arbitrary code.

The gateways are not affected by all vulnerabilities:

| | |
|---|---|
| G430 | CVE-2019-12256 and CVE-2019-12260 only affect G430s with hardware version 3.<br>CVE-2019-12257 and CVE-2019-12264 have no impact because the VxWorks DHCP client is not used.<br>CVE-2019-12262 has no impact because RARP packets are not forwarded to the VxWorks network stack |
| G450 | CVE-2019-12256 and CVE-2019-12260 have no impact because the affected VxWorks version is not used.<br>CVE-2019-12257 and CVE-2019-12264 have no impact because the VxWorks DHCP client is not used<br>CVE-2019-12262 has no impact because RARP packets are not forwarded to the VxWorks network stack |

## Resolution

Avaya has released new Generally Available firmware images to address these vulnerabilities in the VxWorks software:

- 7.1.3.4 loads 39.28.0 (Global) / 39.28.30 (Russian Market only) or later for R7.1.X
- 8.0.1.2 loads 40.31.0 (Global) / 40.31.30 (Russian Market only) or later for R8.0.X
- 8.1.0.1 loads 41.10.0 (Global) / 41.10.30 (Russian Market only) or later for R8.1.X

### Workaround or alternative remediation

An alternateve to updating to the above firmware versions, Avaya recommends following networking and security best practices by implementing firewalls, ACLs, physical security or other appropriate access restrictions to protect themselves from these vulnerabilities.

For applications where devices reside behind a firewall, the "TCP Urgent Pointer" vulnerabilities can be mitigated via the firewall. Administrators can add a rule to drop/block any TCP segment where the URG flag is set.

IP packets with options (that can affect the G430 hardware version 3) can also blocked with an internal gateway access control list, for example:

```
G430v3-011(super)# ip access-control-list 301
G430v3-011(super-ACL 301)# ip-option-in Deny
G430v3-011(super-ACL 301)# exit
G430v3-011(super)# interface Vlan 1
G430v3-011(dev-if:Vlan 1)# ip access-group 301 in
```

To determine if the G430 is hardware version 3, you can use the Communication Manager ‘list media-gateway’ command or the ‘show system’ CLI command on the gateway.

### Remarks

n/a

### Backup before applying the patch

n/a

### Download

n/a

### Patch install instructions

Service-interrupting?

n/a

No

### Verification

n/a

### Failure

n/a

### Patch uninstall instructions

n/a

## Security Notes

The information in this section concerns the security risk, if any, represented by the topic of this PSN.

### Security risks

n/a

### Avaya Security Vulnerability Classification

Not Susceptible

### Mitigation

n/a

**If you require further information or assistance please contact your Authorized Service Provider, or visit support.avaya.com. There you can access more product information, chat with an Agent, or open an online Service Request. Support is provided per your warranty or service contract terms unless otherwise specified in the Avaya support Terms of Use.**

WITH THE INFORMATION OR RECOMMENDED ACTIONS PROVIDED HEREIN, INCLUDING DIRECT, INDIRECT, CONSEQUENTIAL DAMAGES, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF AVAYA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE INFORMATION PROVIDED HERE DOES NOT AFFECT THE SUPPORT AGREEMENTS IN PLACE FOR AVAYA PRODUCTS. SUPPORT FOR AVAYA PRODUCTS CONTINUES TO BE EXECUTED AS PER EXISTING AGREEMENTS WITH AVAYA.