# Multiple IP vulnerabilities in Hirschmann HiOS and Classic Firewall and GarrettCom DX products (URGENT/11)

Date: September 05, 2019
Version: 1.1
References: CVE-2019-12256, CVE-2019-12257, CVE-2019-12255, CVE-2019-12260, CVE-2019-12261, CVE-2019-12263, CVE-2019-12258, CVE-2019-12259, CVE-2019-12262, CVE-2019-12264, CVE-2019-12265

## Summary

The following vulnerabilities in our underlying Wind River VxWorks network stack affect the entire functionality in several versions of the products listed in the next section. Successful exploitation may have an impact on operation or in the worst case an attacker can take control of the system.

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

## Affected Products

| Brand | Product Line / Platform | Product | Version |
|---|---|---|---|
| Hirschmann | HiOS | RSP, RSPE, RSPS, RSPL, MSP, EES, EESX, GRS, OS, RED | 07.0.07 and lower |
| | | MSP40, OS3 | 07.5.01 and lower |
| | | RSPE TSN | 07.3.01 and lower |
| | | DRAGON MACH 4x00 | 07.2.04 and lower |
| | Classic Firewall | EAGLE, EAGLE One | 05.3.06 and lower |
| GarrettCom | DX | DX940e | 1.0.1 Y7 and lower |

## Solution

Belden is currently finalizing updates to address the vulnerabilities. Customers are advised to check our support center for availability of the following versions and to update their products as soon as possible:

| Brand | Product Line / Platform | Product | Version |
|---|---|---|---|
| Hirschmann | HiOS | RSP, RSPE, RSPS, RSPL, MSP, EES, EESX, GRS, OS, RED | 07.0.08 |
| | | MSP40, OS3 | 07.5.02 |
| | | RSPE TSN | 08.0.01 (release pending) |
| | | DRAGON MACH 4x00 | 07.2.05 |
| | Classic Firewall | EAGLE, EAGLE One | 05.3.07 (release pending) |
| GarrettCom | DX | DX940e | 1.0.2 Y2 |

For a temporary solution, customers are advised to use firewalls to block IP traffic reaching affected products or ensure that only trusted IP traffic is passing through affected products.

## For Help or Feedback

To view all Belden Security Advisories and Bulletins or to report suspected security vulnerabilities, go to https://www.belden.com/security.
For technical support and other requests, please visit https://hirschmann-support.belden.com and https://garrettcom-support.belden.com.

## Related Links

[1] Wind River SECURITY VULNERABILITY RESPONSE INFORMATION TCP/IP Network Stack (IPnet, Urgent/11) *(visited 2019-09-05)* https://www.windriver.com/security/announcements/tcp-ip-network-stack-ipnet-urgent11/
[2] 11 Zero Day Vulnerabilities Impacting VxWorks, the Most Widely Used Real-Time Operating System (RTOS) *(visited 2019-09-05)* https://armis.com/urgent11/

## Disclaimer



## Revisions

V1.0 (July 29, 2019): Bulletin published.
V1.1 (September 05, 2019): Bulletin updated (related links, solution).