



Topic: Multiple IP vulnerabilities “Urgent/11 update “in Eagle One Firewall equipment

Dear Valued Customer,

Summary:

The following vulnerabilities in our underlying Win River VxWorks network stack is most likely affecting the entire functionality in versions of the Eagle One Firewall listed below. Details of these vulnerabilities are available from US-CERT in the [ICS-CERT Advisory ICSCA](#). Additional details are available from Wind River’s [Security Advisory](#) and from [Belden Industrial Devices](#).

The product affected are:

- INDUSTRIAL SECURITY ROUTER EAGLEONE TXTX
- INDUSTRIAL SECURITY ROUTER EAGLEONE TXMM
- INDUSTRIAL SECURITY ROUTER EAGLEONE MMTX

We have identified that the system we have provided to you (DCS, TGC, AVR) has potentially one of these products and can be affected by minimum one of the following vulnerabilities.



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

CVSSv is the common vulnerability scoring system from the NIST more information on this site: <https://nvd.nist.gov/vuln-metrics/cvss>

For this affected product GE strongly recommend updating your firmware to a 05.3.07 release or higher, **available on demand on the web site belden.com in the support section.**

Defense in depth

To minimize the risk of exposure to vulnerability's, GE recommend implementing defense in depth strategy for critical process control system.

GE Power Automation & Control Contact information

We can propose on demand a site intervention for equipment's updating, also we will be please to support the enhancement of the cyber security of your system with improved solution. We can conduct a thorough analysis of your cyber security need stop define the optimal solution. If you would like to assess the level of your cybersecurity level, please contact us



GE
Steam Power
Power Automation & Controls

Contact your GE Power Automation & Controls sales person or our Help Desk at +33 1 60 13 43 91 / helpdesk.control-systems@ge.com for help on ordering or cybersecurity services.