GE
Steam Power
Automation & Controls

October 21st, 2019	CYBERSECURITY	ALSPA SYSTEM

Topic: Multiple IP vulnerabilities "Urgent/11 "in CE1500 Equipment

Dear Valued Customer,

Summary:

The following vulnerabilities in our underlying Win River VxWorks network stack is most likely affecting the entire functionality in version of the CE1500 listed below.

Details of these vulnerabilities are available from US-CERT in the ICS-CERT Advisory ICSA. Additional details are available from Wind River's Security Advisory and from BR Automation

The product affected is:

- CE1500 V2 with Atom Processor

We have identified that the system we have provided to you (DCS, TGC, AVR) has potentially this product 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 we are still under evaluation to determine the appropriate next steps.

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
Steam Power
Power Automation & Controls

GE Power Automation & Control Contact information

We will be please to support the enhancement of the cyber security of your equipment with improved solution. We can conduct a thorough analysis of your cyber security need in order to define the optimal solution. If you would like to assess the level of your protection against cyber attacks, please contact us.

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.

Hugues Moreau
Product Manager Power Automation & Controls, GE Steam Power
Hugues.moreau@ge.com