PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg, Germany
Telefon: +49 5235 300
Telefax: +49 5235 3-41200
Internet: http://www.phoenixcontact.com
USt-Id-Nr.: DE124613250
WEEE-Reg.-Nr.: DE50738265

PHOENIX CONTACT GmbH & Co. KG · 32825 Blomberg

20 February 2020
300462894/pbsa56

Security Advisory for FL Switch GHS articles utilizing VxWorks

Advisory Title

Vulnerabilities in the Interpeak IP-stack used in Wind River VxWorks.

Advisory ID

VDE-2020-002
CVE-2019-12255 (TCP Urgent Pointer)
CVE-2019-12258 (DoS via malformed TCP options)

Vulnerability Description

CVS-2019-12255
Wind River VxWorks has a Buffer Overflow in the TCP component (issue 1 of 4). This is an IPNET security vulnerability: TCP Urgent Pointer = 0 that leads to an integer underflow.

The vulnerability affects a little-known feature of the TCP/IP protocol, sending out-of-band data, also known as urgent data. Although the feature is rarely used in the real world, its implementation, consisting of an “Urgent Flag” and an “Urgent Pointer”, is present in the header of every TCP packet. Exploiting these vulnerabilities does therefore not depend on any specific configuration. If a VxWorks device communicates using the TCP protocol, it is vulnerable. It also does not matter which side initiates a TCP connection. An attacker can exploit the vulnerabilities if the VxWorks device is operated as a server that accepts TCP connections, if the VxWorks device connects to a malicious host operated by the attacker, or as a man-in-the-middle, manipulating a TCP connection between the VxWorks device and a legitimate host.

CVE-2019-12258

This vulnerability affects established TCP sessions. An attacker who can figure out the source and destination TCP port and IP addresses of a session can inject invalid TCP segments into the flow, causing the TCP session to be reset.

Affected products

Article no	Article	Affected versions
2700271	FL Switch GHS 4G/12	<= 3.3.0
2700786	FL Switch GHS 4G/12-L3	<= 3.3.0
2700787	FL Switch GHS 12G/8-L3	<= 3.3.0
2989200	FL Switch GHS 12G/8	<= 3.3.0

Impact

CVS-2019-12255
An attacker can either highjack an existing TCP session and inject bad TCP segments, or establish a new TCP session on any TCP port the victim system listens to.
The impact of the vulnerability is a buffer overflow of up to a full TCP receive-window.

CVE-2019-12258
This vulnerability affects established TCP sessions. An attacker who can figure out the source and destination TCP port and IP addresses of a session can inject invalid TCP segments into the flow, causing the TCP session to be reset.

Classification of Vulnerability

CVS-2019-12255
Base Score: 9.8
Vector: CVSS: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVE-2019-12258
Base Score: 7.5
Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Temporary Fix / Mitigation

Users are strongly recommended to install a firewall between the FL Switch GHS device and other parts of the network where an attacker may reside. The firewall needs to be configured in a way that either TCP packets with urgent flag are dropped or that the corresponding TCP connection the packet belongs to is terminated.
It needs to be noticed that the urgent flag is a very rarely used feature. Thus, implementing the described firewall rule will most likely not harm usual network operation.

...

Phoenix Contact recommends operating network-capable devices in closed networks or protected with a suitable firewall. For detailed information on our recommendations for measures to protect network-capable devices, please refer to our application note:

Art.-Nr. 107913: AH EN INDUSTRIAL SECURITY “Measures to protect network-capable devices with Ethernet connection against unauthorized access”

Please also refer to our whitepaper regarding Urgent/11.

Acknowledgement

The vulnerabilities in VxWorks were published by Wind River Systems, Inc.