Cybersecurity Advisory

Wind River VxWorks IPNet Vulnerabilities, impact on Modular Switchgear Monitoring (MSM)

PGVU-PGHV-MSM-2GHV057195

Notice

Affected Products and versions

- MSM CCM, firmware version 2.0.2 and lower

Vulnerability ID

ABB ID: PGVU-PGHV-MSM-2GHV057195

CVE ID: CVE-2019-12256, CVE-2019-12258, CVE-2019-12260, CVE-2019-12261, CVE-2019-12262 and CVE-2019-12263.

Summary

On the 29th of July 2019, a series of vulnerabilities from Wind River affecting the VxWorks operating system were made public. The MSM CCM is affected by some of these vulnerabilities, which are listed above.

An attacker who successfully exploits these vulnerabilities could hijack existing TCP sessions to inject packets of their choosing or cause Denial of Service (DoS) attacks.

Urgent/11 vulnerability consists of 11 individual vulnerabilities. The MSM CCM series is only affected by the eight vulnerabilities listed in the previous section. CVE-2019-12256, CVE-2019-12258, CVE-2019-12260, CVE-2019-12261, CVE-2019-12262 and CVE-2019-12263.

Vulnerability Severity

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) v3. The CVSS Environmental Score, which can affect the vulnerability severity, is not provided in this advisory since it reflects the potential impact of a vulnerability within the end-user organizations' computing environment; end-user organizations are therefore recommended to analyze their situation and specify the Environmental Score.

CVE-2019-12256 Stack overflow in the parsing of IPv4 packets' IP options

CVSS v3 Base Score:	9.8
CVSS v3 Temporal Score:	6.5
CVSS v3 Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CVSS v3 Link:	https://www.first.org/cvss/calculator/3.1

CVE-2019-12258 DoS of TCP connection via malformed TCP options

CVSS v3 Base Score:	7.5
CVSS v3 Temporal Score:	6.5
CVSS v3 Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CVSS v3 Link:	https://www.first.org/cvss/calculator/3.1

CVE-2019-12260 TCP Urgent Pointer state confusion caused by malformed TCP AO option

CVSS v3 Base Score:	9.8
CVSS v3 Temporal Score:	6.5
CVSS v3 Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CVSS v3 Link:	https://www.first.org/cvss/calculator/3.1

CVE-2019-12261 TCP Urgent Pointer state confusion during connect() to a remote host

CVSS v3 Base Score:	8.8
CVSS v3 Temporal Score:	4.4
CVSS v3 Vector:	AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CVSS v3 Link:	https://www.first.org/cvss/calculator/3.1

CVE-2019-12262 Handling of unsolicited Reverse ARP replies (Logical Flaw)

CVSS v3 Base Score:	7.1
CVSS v3 Temporal Score:	4.3
CVSS v3 Vector:	AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:L/E:P/RL:O/RC:C
CVSS v3 Link:	https://www.first.org/cvss/calculator/3.1

CVE-2019-12263 TCP Urgent Pointer state confusion due to race condition

CVSS v3 Base Score:	8.1
CVSS v3 Temporal Score:	5.3
CVSS v3 Vector:	AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CVSS v3 Link:	https://www.first.org/cvss/calculator/3.1

Vulnerability Details

MSM CCM uses the TCP/IP stack from the VxWorks operating system. The vulnerabilities that exist in the VxWorks operating system are included in the product versions listed above. An attacker who successfully exploits these vulnerabilities could hijack existing TCP sessions to inject packets of their choosing or cause Denial of Service (DoS) attacks.

CVE-2019-12256: Stack overflow in the parsing of IPv4 packets' IP options

By sending IPv4 packet with specially crafted options, an attacker could cause a crash of the network task or execute arbitrary code.

CVE-2019-12258: DoS of TCP connection via malformed TCP options

By sending TCP packets with crafted TCP options, an attacker could cause the TCP-session to be reset, triggering a Denial-of-Service condition.

CVE-2019-12260: TCP Urgent Pointer state confusion caused by malformed TCP AO option

By sending TCP packets with malformed TCP's Urgent Point field, an attacker could potentially trigger a crash of the application or execute arbitrary code.

CVE-2019-12261 TCP Urgent Pointer state confusion during connect() to a remote host

By sending TCP packets with malformed TCP's Urgent Point field, an attacker could potentially trigger a crash of the application or execute arbitrary code.

CVE-2019-12262 Handling of unsolicited Reverse ARP replies (Logical Flaw)

An attacker with access to the network, could send reverse-ARP responses to the device. This vulnerability will not cause any harm more than increased usage of RAM. However, it could affect the availability of the device.

CVE-2019-12263 TCP Urgent Pointer state confusion due to race condition

By sending TCP packets with malformed TCP's Urgent Point field, an attacker could potentially trigger a race condition which could lead to execute arbitrary code.

Recommended immediate actions

The issue is corrected in the following product version:

- MSM CCM, firmware version 2.1.0

Hitachi ABB Power Grids recommends that customers apply the update at the earliest convenience.

Mitigation Factors

Recommended security practices and firewall configurations can help protect an industrial network from attacks that originate from outside the network. Such practices include that protection, control & automation systems are physically protected from direct access by unauthorized personnel, have no direct connections to the Internet, and are separated from other networks by means of a firewall system that has a minimal number of ports exposed, and others that have to be evaluated case by case. Protection, control & automation systems should not be used for Internet surfing, instant messaging, or receiving e-mails. Portable computers and removable storage media should be carefully scanned for viruses before they are connected to a control system. Block all non-trusted IP communications.

Workarounds

If an update of the devices is not possible for the operator, a workaround is to restrict access to the devices to only trusted parties/devices.

Frequently Asked Questions

1. **What is the scope of the vulnerability?**
   An attacker who successfully exploited these vulnerabilities could affect communication on the Network.
2. **What causes the vulnerability?**
   The vulnerability is caused by insufficient input data validation in the TCP/IP stack in VxWorks used in MSM CCM.
3. **What is VxWorks and what is the TCP/IP stack?**
   VxWorks is the real time operating system used by MSM CCM. It includes e.g. the TCP/IP stack which is the SW component handling the network communication. IPNet is the name of the TCP/IP stack used in the affected product version.
4. **What might an attacker use the vulnerability to do?**
   An attacker who successfully exploited this vulnerability could disrupt ongoing communication or block new communication on the Network.
5. **How could an attacker exploit the vulnerability?**
   An attacker could try to exploit the vulnerability by creating specially crafted messages and sending the message to an affected controller. For some of the messages this would require that the attacker has direct access to the Network. For others the attack could additionally also be done through a wrongly configured or penetrated firewall. An attack could also be done by installing malicious software on a system node or

otherwise infect the network with malicious software. Recommended practices help mitigate such attacks, see section Mitigating Factors above.

6. **Could the vulnerability be exploited remotely?**
   Yes, an attacker who has network access to an affected system node could exploit this vulnerability. Recommended practices include that process systems are physically protected, have no direct connections to the Internet, and are separated from other networks by means of a firewall system that has a minimal number of ports exposed.
7. **What does the update do?**
   These corrections remove the vulnerability by applying security updates from Wind River that modify the way that the TCP/IP stack validates messages. The network security protection measures are also extended.
8. **When this security advisory was issued, had this vulnerability been publicly disclosed?**
   The list of vulnerabilities in VxWorks has been publicly disclosed by Wind River. Hitachi ABB Power Grids has published the Cybersecurity Notification.
9. **When this security advisory was issued, had Hitachi ABB Power Grids received any reports that this vulnerability was being exploited?**
   No, Hitachi ABB Power Grids had not received any information indicating that this vulnerability had been exploited when this security advisory was originally issued

References

Information from WindRiver about the VxWorks vulnerabilities is available here:
https://www.windriver.com/security/announcements/tcp-ip-network-stack-ipnet-urgent11/

Acknowledgements

Hitachi ABB Power Grids thanks the following for working with us to help protect customers:

Wind River for providing patches and remediation recommendations to address the vulnerabilities pre-sent in their software.

Support

For additional information and support please contact your product provider or Hitachi ABB Power Grids service organization. For contact information, see https://www.hitachiabb-powergrids.com/contact-us/ for Hitachi ABB Power Grids contact-centers.