Cybersecurity Advisory

Libssh server-side vulnerability, impact on XMC20 Multiservice-Multiplexer

PGVU-PGGA-XMC20-2020034

Notice

Affected Products and versions

XMC20 R4 using COGE5 versions older than co5ne_r1h07_12.esw
XMC20 R6 using COGE5 versions older than co5ne_r2d14_03.esw

Vulnerability ID

PG ID: PGVU-PGGA-XMC20-2020034

CVE ID: CVE-2018-10933

Summary

Hitachi ABB Power Grids is aware of public reports of a vulnerability in the product versions listed above. An update is available that resolves a publicly reported vulnerability in the product versions listed above.

An attacker who successfully exploited this vulnerability could remotely take control of the product.

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.

CVSS v3 Base Score:	9.1
CVSS v3 Temporal Score:	8.7
CVSS v3 Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
CVSS v3 Link:	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-10933
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2018-10933

Vulnerability Details

A vulnerability exists in the libssh library included in the product versions listed above. An attacker could exploit the vulnerability by sending a specially crafted message to the XMC20 node, causing the node to allow the attacker to open a communication channel without first performing authentication, resulting in unauthorized access.

Recommended immediate actions

Hitachi ABB Power Grids has corrected the problem in the following product versions:

XMC20 R4: COGE5 version co5ne_r1h07_12.esw (and newer)

XMC20 R6: COGE5 version co5ne_r2d14_03.esw (and newer)

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

Mitigation Factors

Recommended security practices and firewall configurations can help protect a process control network from attacks that originate from outside the network. Such practices include that process control 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. Process control systems should not be used for Internet browsing, 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.

Workarounds

No workarounds have been identified by the vendor.

Frequently Asked Questions

What causes the vulnerability?

The vulnerability is caused by a vulnerability existing in the libssh library included in the products listed above.

What is the affected product?

The products listed above are the COGE5 modules used for managing the whole XMC20 Multiservice-Multiplexer.

What might an attacker use the vulnerability to do?

An attacker could exploit the vulnerability causing the node to allow the attacker to open a communication channel without first performing authentication, resulting in unauthorized access. This may be leveraged to change the operation of the XMC20 node.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by creating a specially crafted message and sending the message to an affected system node. This would require that the attacker has access to the system network, by connecting to the network either directly or through a wrongly configured or penetrated firewall, or that he installs malicious software on a system node or otherwise infects the network with malicious software. Recommended practices help mitigate such attacks, see section Mitigating Factors above.

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 control 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.

What does the update do?

The update removes the vulnerability by using a version of libssh library where the vulnerability is fixed.

When this security advisory was issued, had this vulnerability been publicly disclosed?

Yes, this vulnerability has been publicly disclosed.

When this security advisory was issued, had ABB 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.

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.