TCP Predictability Vulnerability in RTU500 series

ABB-VU-PGGA-1KGT090284

Notice

The information in this document is subject to change without notice, and should not be construed as a commitment by ABB.

ABB provides no warranty, express or implied, including warranties of merchantability and fitness for a particular purpose, for the information contained in this document, and assumes no responsibility for any errors that may appear in this document. In no event shall ABB or any of its suppliers be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, or from the use of any hardware or software described in this document, even if ABB or its suppliers have been advised of the possibility of such damages.

Affected Products

RTU500 series firmware of release 11.3.x and less.

RTU500 series firmware of release 10.x are not affected

Summary

In the operation system used by the device (VxWorks) has a weakness in the random number generator of the TCP implementation may allow remote attackers to predict the correct TCP ISN (Initial Sequence Number) from previous values. This vulnerability affects the product versions listed above.

Additional Information can be found here:

- https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2001-0328
- https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-3963

This vulnerability could be exploited remotely. Successful exploitation of this vulnerability may allow an attacker to spoof or disrupt TCP connections of the affected products.

Severity rating

The severity rating for this vulnerability is important, with the overall CVSS score 5.8. This assessment is based on the types of systems that are affected by the vulnerability, how difficult it is to exploit, and the effect that a successful attack exploiting the vulnerability could have.

CVSS Overall Score: 5.8

CVSS Vector: *(AV:N/AC:M/Au:N/C:P/I:N/A:P)*

CVSS Link:

https://nvd.nist.gov/cvss/v2-calculator?name=CVE-2015-3963&vector=(AV:N/AC:M/Au:N/C:P/I:N/A:P)

Corrective Action or Resolution

ABB has investigated this vulnerability and have now released a maintenance release in order to provide adequate protection to customers. ABB have issued a maintenance release for the affected RTU500 series firmware that will fix this issue.

Affected product version	Version where issue is mitigated
11.3.x and less	Solved in 11.4.1

Based on the customers risk assessment and exposure of the system, the maintenance release should be applied.

ABB recommends that customers also follow the steps outline in the section “Mitigating Factors”.

Customers shall contact their local ABB contacts to obtain the maintenance release.

Vulnerability Details

Affected products generate predictable TCP Initial Sequence Numbers which may allow an attacker to predict the correct TCP ISN and used to spoof or disrupt TCP connections of the affected products.

Mitigating Factors

Recommended security practices and firewall configurations can help protect an industrial control network from attacks that originate from outside the network. Such practices include

that industrial 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. Industrial control 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.

Workarounds

Workarounds are described in the *Corrective Action or Resolution* chapter above.

Frequently asked questions

What is the scope of the vulnerability?
An attacker who successfully exploits this vulnerability could spoof or disrupt TCP connections of the affected products.

What causes the vulnerability?
This vulnerability is caused by a weakness in the TCP random number generator algorithm implemented in the operating system (VxWorks) used by the RTU500 series.

What is the affected product or component?
In the RTU500 series, the affected parts are the HTTP/HTTPS used for web based access and all available protocols using TCP, like IEC 60870-5-104, DNP3.0 LAN/WAN, Modbus TCP, etc. All protocols uses the TCP stack implemented by the operating system (VxWorks).

What might an attacker use the vulnerability to do?
An attacker who successfully exploits this vulnerability could spoof or disrupt protocol connections or web based access connections of the affected products.

How could an attacker exploit the vulnerability?
An attacker could try to exploit this vulnerability. It 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 industrial 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.

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, ABB had not received any information indicating that this vulnerability had been exploited in the RTU500 series when this security advisory was originally issued.

Support

For additional information and support please contact your local ABB service organization. For contact information, see www.abb.com/substationautomation.

Information about ABB's cyber security program and capabilities can be found at www.abb.com/cybersecurity.