DOCUMENT ID: 7PAA001353
REVISION: B
DATE: 2022-04-08
SECURITY LEVEL: PUBLIC

CYBER SECURITY ADVISORY

SECURITY – Denial of Service Vulnerabilities in SPIET800 INFI-Net to Ethernet Transfer module and PNI800 S+ Ethernet communication interface module

CVE ID: CVE-2021-22285, CVE-2021-22286, CVE-2021-22288

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.

This document and parts hereof must not be reproduced or copied without written permission from ABB, and the contents hereof must not be imparted to a third party nor used for any unauthorized purpose.

All rights to registrations and trademarks reside with their respective owners.

Purpose

ABB has a rigorous internal cyber security continuous improvement process which involves regular testing with industry leading tools and periodic assessments to identify potential product issues. Occasionally an issue is determined to be a design or coding flaw with implications that may impact product cyber security.

When a potential product vulnerability is identified or reported, ABB immediately initiates our vulnerability handling process. This entails validating if the issue is in fact a product issue, identifying root causes, determining what related products may be impacted, developing a remediation, and notifying end users and governmental organizations (e.g. ICS-CERT).

The resulting Cyber Security Advisory intends to notify customers of the vulnerability and provide details on which products are impacted, how to mitigate the vulnerability or explain workarounds that minimize the potential risk as much as possible. The release of a Cyber Security Advisory should not be misconstrued as an affirmation or indication of an active threat or ongoing campaign targeting the products mentioned here. If ABB is aware of any specific threats, it will be clearly mentioned in the communication.

The publication of this Cyber Security Advisory is an example of ABB's commitment to the user community in support of this critical topic. Responsible disclosure is an important element in the chain of trust we work to maintain with our many customers. The release of an Advisory provides timely information which is essential to help ensure our customers are fully informed.

Affected products

ABB Ability™ Symphony® Plus:

– SPIET800 - INFI-Net to Ethernet Transfer Module: All firmware versions A_B or earlier are affected.

– PNI800 – S+ Ethernet communication interface module: All firmware versions A_B or earlier are affected.

Vulnerability IDs

CVE-2021-22285, CVE-2021-22286, CVE-2021-22288

Summary

Multiple vulnerabilities were privately reported relating to ABB's implementation of the SPIET800 used in some ABB Process Automation control systems. The same vulnerabilities are also affecting the ABB PNI800 devices.

If an attacker gains access to a site's control network, then exploiting these vulnerabilities will result in a denial-of-service situation for such ABB devices and will require a manual restart.

The unavailability of the SPIET800 or PNI800 devices would prevent data transactions by the connected Operations and Engineering workstations but would not affect the system configuration data, nor the INFI-Net or PN800 control network.

Recommended immediate actions

ABB advises all customers to review their installations to determine if they are using an impacted product as listed above.

- SPIET800 devices with firmware version A_B or earlier are affected. All the vulnerabilities will be corrected in version A_C or later (planned Q2 2022).
- PNI800 devices with firmware version A_B or earlier are affected. All the vulnerabilities will be corrected in version B_0 or later (planned Q2 2022).

End users who are unable to install one of these updates should immediately look to implement the Mitigation and Workarounds listed below as this will restrict or prevent an attacker's ability to compromise these systems.

ABB recommends that customers apply the update at earliest convenience.

Vulnerability severity and details

Multiple vulnerabilities exist in the packet handling of the SPIET800/PNI800 communication stack included in the product revisions listed above. An attacker could exploit these vulnerabilities by using a specially crafted message or sending an incomplete (Out of Order) sequence of packets, forcing the communication Interface (SPIET800 or PNI800 devices) to be unresponsive, resulting in a denial-of-service situation and requiring a manual reboot.

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) v3.1[1].

CVE-2021- 22285 – Incorrect Handling of OoO Packets

During normal operation, sequence of packets can be exchanged in an ABB DCS system via an SPIET800 or PNI800 device. Errors in handling OoO packets may cause the device to stop responding to any Ethernet-based requests. The denial of service would not self-resolve, requiring a reboot to restore normal operation.

CVSS v3.1 Base Score:	7.5 High
CVSS v3.1 Temporal Score:	7.2 High
CVSS v3.1 Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:H/RL:T/RC:C
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2021-22285

CVE-2021- 22286 - Malformed Packet Handling

During communications with the SPIET800 or PNI800 device it was observed that formatting the IET protocol packet with some invalid values would cause the devices to become unresponsive. The denial of service would not self-resolve, requiring a reboot to restore normal operation.

CVSS v3.1 Base Score:	7.5 High
CVSS v3.1 Temporal Score:	7.2 High

[1] 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 v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:H/RL:T/RC:C
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2021-22286

CVE-2021- 22288 - Unresponsive after TCP scan

During device evaluation of an ABB DCS device with an SPIET800/PNI800, it was observed that certain types of unexpected traffic cause the device to become unresponsive. The denial of service would not self-resolve, requiring a reboot to restore normal operation.

CVSS v3.1 Base Score: 7.5 High
CVSS v3.1 Temporal Score: 7.2 High
CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:H/RL:T/RC:C
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2021-22288

Mitigating factors

Any exploit of this vulnerability would require that the attacker has access to the control network. Following ABB's recommended security practices including network architecture and perimeter firewall are mitigating factors in preventing external access to the control network.

Refer to section "General security recommendations" for further advice on how to keep your system secure.

Workarounds

No workarounds are available. Assess the installation specific risk based on this advisory. Use the recommendations described under "Mitigating factors" and "Recommended immediate actions".

Frequently asked questions

What is the scope of the vulnerability?

An attacker who successfully exploited this vulnerability could remotely cause the SPIET800 or PNI800 device to stop (denial of service). While the SPIET800 and PNI800 are directly impacted and will fault, it should be noted that systems connected to the SPIET800 or PNI800 will be impacted by the inability to transact with these devices.

What causes the vulnerability?

The vulnerability is caused by an incorrect handling of either the sequence of packets (Out of Order packets) or malformed packet fields in the SPIET800 and PNI800 devices.

What is the SPIET800?

The SPIET800 is an INFI-NET-to-Ethernet module which enables communication between the INFI-NET control network and a host computer running an engineering tool (e.g., S+ Engineering), an HSI (e.g., S+ Operations or 800xA for Symphony Plus Harmony), or a general purpose interface (e.g., Harmony OPC Server).

What is the PNI800?

The PNI800 is a communication interface between the PN800 control network and a host computer running an engineering tool (e.g., S+ Engineering), an HSI (e.g., S+ Operations or 800xA for Symphony Plus Harmony), or a general purpose interface (e.g., Harmony OPC Server).

What might an attacker use the vulnerability to do?

An attacker can use the vulnerability to cause a denial-of-service situation which could affect the online activities of the connected S+ Operations and Engineering.

How could an attacker exploit the vulnerability?

To exploit the vulnerability an attacker would need to get local access to control network or have remote access to a system server. With that access gained the attacker would need to send a specially crafted message to IP address of an SPIET800 or PNI800. That message could halt the IET/PNI component which would no longer respond to data transfer request from the Operator network which can be describe as a Denial of Service condition.

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.

Can functional safety be affected by an exploit of this vulnerability?

Functional safety systems are not affected by these vulnerabilities.

What does the update do?

The updates for the SPIET800 and the PNI800 devices remove the vulnerabilities by improving the processing of received TCP packets.

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

No, ABB received information about this vulnerability through responsible disclosure.

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 when this security advisory was originally issued.

General security recommendations

Control systems and the control network are exposed to cyber threats. In order to minimize these risks, the protective measures and best practices listed below are available in addition to other measures. ABB strongly recommends system integrators and asset owners to implement the measures they consider appropriate for their control system environment:

– Place control systems in a dedicated control network containing control systems only.

- Locate control networks and systems behind firewalls and separate them from any other networks like business networks and the Internet.
- Block any inbound Internet traffic destined for the control networks/systems. Place remote access systems used for remote control system access outside the control network.
- Limit outbound Internet traffic originating from control systems/networks as much as possible. If control systems must talk to the Internet, tailor firewall rules to required resources - allow only source IPs, destination IPs and services/destination ports which control systems definitely need to use for normal control operation.
- If Internet access is required on occasion only, disable relevant firewall rules and enable them during the time window of required Internet access only. If supported by your firewall, define an expiry date and time for such rules – after the expiry date and time, the firewall will disable the rule automatically.
- Limit exposure of control networks/systems to internal systems. Tailor firewall rules allowing traffic from internal systems to control networks/systems to allow only source IPs, destination IPs and services/destination ports which are definitely required for normal control operation.
- Create strict firewall rules to filter malicious network traffic targeting control system vulnerabilities ("exploit traffic"). Exploit traffic may use network communication features like source routing, IP fragmentation and/or IP tunneling. If such features are not required for normal control operation, block them on your firewall.
- If supported by your firewall, apply additional filters to allowed traffic which provide protection for control networks/systems. Such filters are provided by advanced firewall features like Application Control and Anti-Virus.
- Use Intrusion Detection Systems (IDS) or Intrusion Preventions Systems (IPS) to detect/block control system-specific exploit traffic. Consider using IPS rules protecting against control system exploits.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs). Please ensure that VPN solutions are updated to the most current version available.
- In case you want to filter internal control network traffic, consider using solutions supporting Intra-LAN traffic control like VLAN access control lists.
- Harden your control systems by enabling only the ports, services and software required for normal control operation. Disable all other ports and disable/uninstall all other services and software.
- If possible, limit the permissions of user accounts, software processes and devices to the permissions required for normal control operation.
- Use trusted, patched software and malware protection solutions. Interact with trusted web sites and trusted email attachments only.
- Ensure all nodes are always up to date in terms of installed software, operating system and firmware patches as well as anti-virus and firewall.
- Protect control systems from physical access by unauthorized personnel e.g. by placing them in locked switch cabinets.

More information on recommended practices can be found in the following documents[2]:

[2] Access to some listed documents can be subject to the ABB Care Automation Software Maintenance specific conditions and agreements.

8VZZ001882	S+ Control SPC600/700/800 SD Series controllers user manual
8VZZ001006	Symphony Plus Secure deployment guide for Windows 10 and Server 2016/2019 user manual
2PAA121027	Distributed Control Systems - McAfee® ePO with VirusScan Enterprise, Endpoint Security and Application Control
8VZZ000602	Microsoft Security Updates Validation Status for Symphony Plus
8VZZ001753	McAfee Virus Scan DAT Update Validation Status for Symphony Plus
2PAA122516	System 800xA, Symphony Plus and Freelance System Hardening - End user manual
2PAA120528	System 800xA, Symphony Plus and Freelance System Hardening: Group Policies Overview
8VZZ000368D0066	ICS Cyber Security Reference Architecture Guide

Acknowledgement

ABB thanks Lance Lamont from Verve Industrial Protection and Ron Brash from Verve Industrial Protection/aDolus Technology Inc. helping to identify the vulnerabilities and protecting our customers.

Support

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

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

Revision history

Rev. Ind.	Page (p) Chapter (c)	Change description	Rev. date
A	all	Initial version	12/01/2021
B	page 3	Updated planned release from Q1 to Q2	04/08/2021