DOCUMENT ID: 7PAA002536
REVISION: A
DATE: 2024-03-26
SECURITY LEVEL: PUBLIC

CYBER SECURITY ADVISORY

SECURITY – Denial of Service Vulnerability in Control API ‘VPNI’, impact on S+ Operations, S+ Engineering and S+ Analyst

CVE ID: CVE-2024-0335

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

Product / System line	Products and Affected Versions
S+ Operations	Versions 3.3 SP1 RU4 and earlier are affected. Versions 2.1 SP2 RU3 and earlier are affected. Versions 2.0 SP6 TC6 and earlier are affected.
S+ Engineering	Versions 2.1 through 2.3 RU3 are affected.
S+ Analyst	Versions 7.0.0.0 to 7.2.0.2 using Fast Data Logger are affected. Note: S+ Analyst with Vibration Analysis will not be affected by the Control API VPNI vulnerability because it does not use it.

Vulnerability IDs

CVE-2024-0335

Summary

ABB has internally identified a vulnerability in the ABB VPNI [1] feature of the S+ Control API component which may be used by several Symphony Plus products (e.g., S+ Operations, S+ Engineering and S+ Analyst).

[1] The Virtual PNI (VPNI) is a feature of the Windows-based Control API Runtime software provided with S+ Engineering product.

If an attacker gains access to a site's HMI network, then exploiting this vulnerability will result in a denial-of-service (DoS) of the VPNI, which would prevent data transfer from/to the above affected S+ products that utilize the feature to connect to the HMI network.

The unavailability of the VPNI would prevent data transactions by the connected S+ Operations, S+ Engineering and Analyst workstations but would not affect the system configuration data, nor the Symphony Plus HMI network.

Recommended immediate actions

ABB advises all customers to review their installations to determine if they are using an impacted product as listed above, no further analysis or tools are needed to make this determination. The recommended immediate actions for S+ products using the VPNI feature are listed below:

- **S+ Operations**

  Systems using S+ Operations versions 3.3 SP1 RU4 or earlier should upgrade to version 3.3 SP1 RU5 (planned for Q3 2024) or later.

  Systems using S+ Operations 2.1 SP2 RU3 or earlier should upgrade to version 3.3.1 RU5 (planned for Q3 2024) or later.

  Systems using S+ Operations 2.0 SP6 TC6 or earlier should upgrade to version 3.3 SP1 RU5 (planned for Q3 2024) or later.

- **S+ Engineering**

  Systems using S+ Engineering 2.1 through 2.3 RU3 should upgrade to S+ Engineering 2.4 (released in January 2023) or later.

- **S+ Analyst**

  Systems using S+ Analyst with Vibration Analysis will not be affected by the VPNI problem because it does not use it. Systems using S+ Analyst with the Fast Data Logger versions 7.0.0.0 to 7.2.0.2 should upgrade to version 7.3 (planned for Q2 2024) or later.

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

A vulnerability exists in the VPNI feature included in the product revisions listed above.

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) v3.1[2].

[2] 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-2024-0335 - Malformed Packet Handling

An attacker could exploit the vulnerability by formatting the VPNI protocol packet with some invalid values, causing the VPNI service to be unresponsive (crash), resulting in a denial-of-service situation.

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:O/RC:C
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2024-0335

Mitigating factors

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

Note that to reduce the impact on the VPNI unavailability, the VPNI can be configured to automatically restart after a few minutes (see figure 6.4 in section 6.1 of the "S+ System Virtual PNI installation and configuration user manual", 2VAA003419).

Refer to section "General security recommendations" for the above ABB security practices and 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 VPNI to stop (denial of service). Symphony Plus applications using the VPNI functionalities (affected products are S+ Operations, S+ Engineering and S+ Analyst) will not be able to use the service which has been stopped. This does not affect the other Symphony Plus functionalities, nor the HMI network.

What causes the vulnerability?

The vulnerability is caused by an incorrect handling of invalid values in the VPNI protocol packet.

What is the Virtual PNI (VPNI)?

The Virtual PNI (VPNI) is a feature of the Windows-based Control API Runtime software provided with several S+ products. It is a Control API communications server configured to act as a CIU and provide PN800 connectivity to S+ Operations and Engineering servers and Analyst.

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, Engineering and Analyst.

How could an attacker exploit the vulnerability?

To exploit the vulnerability an attacker would need to get access to the site's HMI network. With that access gained, the attacker would need to send invalid packets to the VPNI service. Those messages could cause the VPNI component to stop (crash) which would no longer respond to data transfer requests from client applications (which can be described as a Denial-of-Service condition).

Could the vulnerability be exploited remotely?

Yes, an attacker who has network access to client/server HMI network 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 affected products remove the vulnerability by improving the VPNI handling of invalid packet values.

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

No, ABB had identified this through an internal evaluation.

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. 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[3]:

2VAA003419	S+ System Virtual PNI installation and configuration 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

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

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	2024/3/26