DOCUMENT ID: 9AKK108467A6732
REVISION: B
DATE: 2023-03-16

CYBER SECURITY ADVISORY

NE843 Pulsar Plus Controller Cyber Security Advisory

CVE ID: CVE-2022-1607, CVE-2022-26080

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.

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

Infinity DC Power Plant – H5692448 G104 G842 G224L G630-4 G451C(2) G461(2) – comcode 150047415

Pulsar Plus System Controller – NE843_S – comcode 150042936

Vulnerability IDs

ABBVREP0035

CVE-2022-1607, CVE-2022-26080

Summary

An update is available that resolves a privately reported vulnerability in the product versions listed above. The update is version number 5.0.0 for the application and 5.0.0 for web pages.

An attacker who successfully exploited this vulnerability could cause the product to stop, make the product inaccessible, take remote control of the product, or insert and run arbitrary code.

The vulnerabilities privately reported include:

1. Poor protection from Cross Site Request Forgery.
2. GET requests that can cause controller state changes.
3. Sessions IDs that can be easily guessed.
4. Session IDs that are visible in URLs.
5. Poor Cross Site Scripting prevention.

The available update resolves these issues.

Recommended immediate actions

The problem is corrected in the following product versions: application 5.0.0 and web pages 5.0.0

ABB recommends that customers apply the update at earliest convenience.

Vulnerability severity and details

A vulnerability exists in the web server included in the product versions listed above. An attacker could exploit the vulnerability by sending a specially crafted message to the system node, allowing the attacker to take control of the product or insert and run arbitrary code.

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

Session ID handling (CVE-2022-26080)

Every interaction with the web server requires a Session ID that is assigned to the session after a successful login. The reported vulnerability is that the Session IDs were too short (16 bits), too predictable (IDs simply incremented), and were plainly visible in the URLs of the web pages. These issues were remediated by rewriting the web server to follow recommended best practices.

CVSS v3.1 Base Score:	6.3
CVSS v3.1 Temporal Score:	5.7
CVSS v3.1 Vector:	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:H/A:N/E:P/RL:O/RC:C
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2022-26080

Cross Site Scripting (CVE-2022-1607)

There are several fields in the web pages where a user can enter arbitrary text such as a description of an alarm or a rectifier. These represent a Cross Site Scripting vulnerability where javascript code can be entered as the description with the potential of causing system interactions unknown to the user. These issues were remediated by adding a check of every field update to reject suspicious entries.

CVSS v3.1 Base Score:	4.6
CVSS v3.1 Temporal Score:	4.2
CVSS v3.1 Vector:	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2022-1607

Mitigating factors

These products are most often used within a firewall protected local area network. Ensure the firewall protection is properly configured.

[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.

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

Workarounds

A workaround is to use the controller’s Read/Write Enable/Disable feature for a network port (NET1,WRE=0). The controller can disable all writes over the network port. The factory default is to have the write capability enabled. However, some customers do not want settings to be remotely changed once systems are set. This feature, when set to Disable, will allow no changes to be accepted. Once set it can only be changed locally through the front panel.

ABB has tested the following workarounds. Although these workarounds will not correct the underlying vulnerability, they can help block known attack vectors. When a workaround reduces functionality, this is identified below as “Impact of workaround”.

Frequently asked questions

What is the scope of the vulnerability?

An attacker who successfully exploited this vulnerability could remotely cause an affected system node to stop or insert and run arbitrary code in an affected system node.

What causes the vulnerability?

The vulnerability is caused by the design of the web server with inadequate handling of Session IDs and unchecked input data.

What is the web server?

The web server is the part of the Pulsar application that responds to HTTP requests from a user’s web browser.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could cause the affected system node to stop or become inaccessible, allow the attacker to take control of the system node, or allow the attacker to insert and run arbitrary code.

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.

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

An attacker that gains super-user or admin level access levels could place rectifiers in standby, causing the system to revert to battery operation. This event would normally be alarmed but the attacker may modify all alarms to Record Only and prevent proper notification.

What does the update do?

The update removes the vulnerability by modifying the way that the web server validates messages and verifies input data.

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

For any installation of software-related ABB products we strongly recommend the following (non-exhaustive) list of cyber security practices:

- Isolate special purpose networks (e.g. for automation systems) and remote devices behind firewalls and separate them from any general purpose network (e.g. office or home networks).
- Install physical controls so no unauthorized personnel can access your devices, components, peripheral equipment, and networks.
- Never connect programming software or computers containing programing software to any network other than the network for the devices that it is intended for.
- Scan all data imported into your environment before use to detect potential malware infections.
- Minimize network exposure for all applications and endpoints to ensure that they are not accessible from the Internet unless they are designed for such exposure and the intended use requires such.
- 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.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs). Recognize that VPNs may have vulnerabilities and should be updated to the most current version available. Also, understand that VPNs are only as secure as the connected devices.

Acknowledgement

We acknowledge the help of Vlad Ionescu of Facebook Red Team X for reports on the vulnerabilities described in this document.

References

Cross-Site Request Forgery Prevention

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	2022-12-27
B	all P3	Updated per Cyber-Security Team comments Added NVD Summary Links	2023-03-16