DOCUMENT ID: 3BHS910120
REVISION: B
DATE: 2023-04-28

CYBER SECURITY ADVISORY

SECURITY - IEC 61850 Communication Stack vulnerability, impact on ABB AC 800PEC and AC 800PEC-based products

CVE ID: CVE-2022-3353

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.

© Copyright 2023 ABB. All rights reserved.

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

Controllers

- AC 800PEC PP D103, PP D104 (PowerPC) 5.0.3.4 and older
- AC 800PEC PP E10x (PowerPC) 5.4.3.0 and older

Products

The following products are affected as being based on the above controllers:

- DT2S - Dynamic Time to Surge Solution, Versions 1.0.0.2 and older
- IEC 61850 Interface for UNITROL 6000 Medium, Versions 2.1.00 and older
- UNITROL 6000 X-power, Versions 6.0.04 and older
- SYNCHROTACT 5, Versions 2.3.1 and older
- SYNCHROTACT 6, Versions 1.1.0.0 and older
- UNIREC for Marines, Versions 3.1.00 and older

Vulnerability IDs

CVE-2022-3353

© Copyright 2023 ABB. All rights reserved.

Summary

ABB is aware of reported vulnerabilities in Hitachi's IEC 61850 communication stack (CVE-2022-3353) that is used in the AC 800PEC and AC 800PEC based-product versions listed in this document. An update for the AC 800PEC controllers will be made available that remediates the identified vulnerabilities during Q4 2023. The affected products will be addressed in parallel, and updates will be released afterwards. This document also describes some mitigations that can help concerned users limit their risk.

An attacker who successfully exploited this vulnerability could force the IEC 61850 MMS-server communication stack to stop accepting new MMS-client connections. A reboot of the AC 800PEC and based-products is required to reenable IEC 61850 MMS-server communication for accepting new MMS-client connections. During the reboot phase, the primary functionality of the AC 800PEC is not available.

Recommended immediate actions

ABB advises all customers to review their installations to determine if they are using an impacted controller or product as listed above, follow the Mitigation Factors listed below, and deploy the upcoming updates when in scope and available.

The vulnerability will be fixed in upcoming AC 800PEC release version 5.4.4.0 during Q4 2023.

Updates to the above-mentioned affected products will be made available subsequently.

Vulnerability severity and details

A vulnerability exists in the IEC 61850 MMS-server communication stack included in the AC 800PEC controllers and in the AC 800PEC-based products listed above. An attacker could exploit the vulnerability by using a specially crafted message sequence to force the IEC 61850 MMS-server communication stack to stop accepting new MMS-client connections. Already existing/established client-server connections are not affected.

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

CVE 2022-3353 and IEC 61850 MMS-Server Vulnerability

CVSS v3.1 Base Score:	5.9 Medium
CVSS v3.1 Vector:	AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2022-3353

[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.

© Copyright 2023 ABB. All rights reserved.

Mitigating factors

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

Frequently asked questions

What is the scope of the vulnerability?

An attacker who successfully exploits this vulnerability can force the IEC 61850 MMS-server communication stack in the listed versions of the AC 800PEC to stop accepting new MMS-client connections. A reboot is required to reenable IEC 61850 MMS-server communication for accepting new MMS-client connections. This vulnerability also impacts several versions of AC 800PEC-based products as listed above.

Note:
Already existing/established client-server connections are not affected (will not be disconnected).
IEC 61850 communication for GOOSE publishing or subscription is not affected. (For products supporting MMS-Server and GOOSE)
IEC 61850 MMS-client communication is not affected. (For products supporting MMS-server and MMS-client communication)

What causes the vulnerability?

The vulnerability is caused by the third-party IEC 61850 communication stack (CVE-2022-3353).

What is AC 800PEC?

The AC 800PEC combines the high-speed control requirements of processes like those in power electronics applications with the low-speed process control tasks usually carried out by separate PLC units.

What is DT2S - Dynamic Time to Surge Solution?

DT2S - Dynamic Time to Surge Solution is an integrated drive and compressor protection system. Embedded Software for AC 800PEC for compressor protection. It reads measurements from electrical and process data and calculates if a shutdown is needed due to a sudden loss of drive torque.

What is UNITROL® 6000?

Specifically designed to serve the needs of generators within steam, gas, nuclear and hydro power plants as well as motors in process industries such as steel mills, pulp and paper, chemical, natural gas production plants and refineries, UNITROL® 6000 for Indirect and Static Excitation comes in three versions - Light, Medium and X-power - serving different current ranges and customization levels.

What is SYNCHROTACT?

The SYNCHROTACT product family is used in power plants, substations, and industrial plants with own power generation. The digital synchronizer can be used for the following applications:

- Automatic synchronization and paralleling of generators
- Automatic paralleling of synchronous and asynchronous lines, transmission lines and busbars
- As a paralleling monitoring device (synchrocheck) to monitor automatic or manual paralleling sequences

© Copyright 2023 ABB. All rights reserved.

What is UNIREC for Marines?

Scalable power rectifier based on a full-wave thyristor converter and ABB control technology. Designed for projects with high requirements in terms of performances and capacities.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could force the IEC 61850 MMS-server communication stack to stop accepting new MMS-client connections. A reboot of the AC 800PEC is required to reenable IEC 61850 MMS-server communication for accepting new MMS-client connections. During the reboot phase, the primary functionality of the controller is not available.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by creating a specially crafted message sequence and sending the message sequence to an affected AC 800PEC. 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 remotely.

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?

No.

Can the core functionality be affected by an exploit of this vulnerability?

No.

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

Yes, this vulnerability has been publicly disclosed as CVE 2022-3353.

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.

© Copyright 2023 ABB. All rights reserved.

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 net-work 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

ABB appreciates the report from Hitachi about CVE 2022-3353.

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	2023-02-21
B	2	Updated affected product versions [UNITROL 6000 Medium, and UNIREC for Marines]	2023-04-28

© Copyright 2023 ABB. All rights reserved.