ABB DOC ID: 8VZZ002158
REVISION: A
DATE: 2019-11-01

CYBER SECURITY ADVISORY

SECURITY Power Generation Information Manager Vulnerability

Vulnerability ID: ABBVU-IAPG-8VZZ002158

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.

Affected Products

Power Generation Information Manager (PGIM) – all versions

Plant Connect - all versions

Vulnerability ID

ABB ID: ABBVU-IAPG-8VZZ002158

Summary

ABB is aware of public reports of a vulnerability in the product versions listed above. An attacker who exploits this vulnerability can bypass authentication and extract the user credentials used within the application. An updated product, Symphony Plus Historian, is available that resolves the publicly reported vulnerabilities.

Vulnerability Severity

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) v3. 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 Base Score:	9.8 (Critical)
CVSS v3 Temporal Score:	9.0 (Critical)
CVSS v3 Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C
CVSS v3 Link:	

https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C

Recommended immediate actions

ABB advises all customers to review their installations to determine if they are using an impacted system in the Affected Products section above. Note ALL versions of PGIM and Plant Connect are affected, no further analysis or tools are needed to make this determination.

Additionally, end-users should immediately look to implement the Mitigation and Workarounds listed below as this will significantly restrict an attacker's ability to compromise these systems.

PGIM will transition to a limited support phase in January 2020. Plant Connect is already obsolete.

Users are advised to upgrade to Symphony Plus Historian as this is not affected. Symphony Plus Historian is the successor of the PGIM and Plant Connect products with improved cyber security. Symphony Plus Historian is now fully based on Windows authentication which avoids exposure to the security issues with PGIM and Plant Connect.

Please note that depending on the PGIM deployment you need to consider the compatibility with connected or integrated products (e.g. Microsoft Operating System, System 800xA versions, 3rd party OPC servers, etc). Customers unable to update to Symphony Plus Historian should reference the Workaround section below for additional advice.

Please refer to the Symphony Plus Historian sales announcement for additional details on compatibility and product migration which can be found by using the Reference section below. For additional support contact your local ABB Service organization.

Vulnerability Details

PGIM uses an approach for user credential management in which applications manage user accounts. These applications were not designed to withstand the techniques that attackers can utilize on exposed networks and endpoints. Therefore, if the network communication or endpoints for these applications are not protected, unauthorized actors can bypass authentication and extract the user credentials used within the applications.

In some cases, end users have used the same usernames and passwords for Windows login and with applications such as PGIM. In such instances, if an un-authorized user extracts credentials for PGIM and Plant Connect, then they would also be in possession of Windows credentials, potentially compromising the security of the Domain.

Mitigating Factors

Recommended baseline security practices and firewall configurations can help protect a network and its attached devices from attacks that originate from outside the network. For example, common practices are for process control systems to be 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 must be evaluated case by case.

Process control and automation systems should not be used for general business functions (e,g. internet browsing, email, etc.) which are not critical industrial processes. Portable computers and removable storage media should be carefully scanned for viruses before they are connected to a control system.

Workarounds

Customers using PGIM are advised not to use the same user credentials for Windows login as used to log into the PGIM and Plant Connect applications. Additionally, end users that cannot immediately upgrade should consider protecting the network communication by use of IPSec or other means. Customers should contact ABB for additional support details.

Frequently Asked Questions

What is the scope of the vulnerability?

The vulnerability is related to an application-based implementation of user management which has a methodology for authentications which does not securely maintain user credentials. Additionally, if the network traffic is not encrypted, user login credentials for PGIM are possible to intercept on the network.

An attacker who successfully exploited these vulnerabilities could cause loss of historical data and events. Additionally, knowledgeable user could obtain administrative privilege and write data to the control platform If the plant control system application has been configured to allow data to be written from the PGIM application.

What causes the vulnerability?

Insufficient protections of user credentials and authentication mechanisms were caused by older technology in the product which could not be updated to best practice methods.

What is Power Generation Information Manager (PGIM)?

PGIM is a plant historian and data analysis tool. It is intended to provide reports, trends and other useful information which can be extracted from the process values collected and stored in the data repository.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could obtain the PGIM user credentials. With this information, the attacker could alter the configuration of the PGIM History and Event database. The result could be loss of plant data collection and inability to collect expected reports.

If users have chosen to use the same user credentials for the PGIM application as they used for Windows login, then an attacker who obtained the PGIM credential could also access Windows resources.

Can an attacker use the vulnerability to impact the plant control system?

If a plant control system application has been configured to allow data to be written from the PGIM historian system, then an attacker may be able to utilize PGIM to send unauthorized data to the plant control system.

How could an attacker exploit the vulnerability?

An attacker with access to the network could try to exploit the vulnerability by “sniffing” traffic and by analyzing the protocol and could obtain user credentials.

Another approach is that an attacker could try to exploit the vulnerability by communicating to the PGIM server with unauthenticated messages. This would require the attacker to have access to the system network, by connecting to the network either directly or through a wrongly configured or penetrated firewall, or that they install 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.

Is there an update that corrects the problem?

Yes, users are advised to upgrade to Symphony Plus Historian v3.1 or later, on supported version of the Windows Operating System where the issues that are addressed by this advisory are fully resolved. Symphony Plus Historian v3.1 or later is the direct migration path for the PGIM 5.1. If the user subscribes to an Automation Sentinel Maintain contract, they may be eligible for the software free of charge. Please contact ABB with additional support details should your system require a custom migration path.

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

Yes, this issue has been publicly presented.

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 maliciously exploited when this security advisory was originally issued. However, exploit code has been made publicly available.

Why is Symphony Plus Historian not affected by this vulnerability? Can it not be configured to use the same vulnerable protocol as PGIM?

A Symphony Plus Historian client by default uses Windows authentication, but it can be configured to use the PGIM protocol for compatibility reasons.

The PGIM vulnerability is a vulnerability in the server. The Symphony Plus Historian server cannot be configured to use the PGIM protocol. This means that the Symphony Plus Historian is not at all affected by this vulnerability.

Acknowledgements

ABB thanks Rikard Bodforss of Bodforss Consulting for helping to bring this item to conclusion

References

Information from Symphony Plus Historian sales release announcements are available here:

2VAA008267-300 Symphony Plus Historian 3.0 Release Note LINK

2VAA008267-310 Symphony Plus Historian 3.1 Release Note LINK

8VZZ001642T5100 Power Generation Information Manager 5.1 Lifecycle Update LINK

Support

For additional instructions and support please contact your local ABB service organization. For contact information, see https://new.abb.com/contact-centers.

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