DOCUMENT ID: 8MAL100030-0015
REVISION: A
DATE: 2023-01-03

CYBER SECURITY ADVISORY

Vulnerabilities in PTC KEPServerEX: Impact on Marine ITMonitoring

CVE ID's: CVE-2022-2825; CVE-2022-2848

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 2022 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

The following product is affected by vulnerabilities found in Kepware KEPServerEX platform:

- Marine ITMonitoring version 1.0.2 and 1.0.3; previous versions of Marine ITMonitoring are not affected.

Marine ITMonitoring is often used in ABBs Integrated Automation, Propulsion Control and Power & Energy Management Systems for monitoring IT equipment and indicating this in HMI displays.

Vulnerability IDs

CVE-2022-2825; CVE-2022-2848

Summary

PTC is the provider of the connectivity platform called KEPServerEX which is used in the Marine ITMonitoring software. PTC has announced the below listed security vulnerabilities in the Kepware KEPServerEX 6.12 and prior which impact the Marine ITMonitoring version 1.0.2 and 1.0.3.

Exploiting these vulnerabilities using a specially crafted OPC UA messages could crash the server and leak data transmitted to that server.

PTC KEPServerEX vulnerabilities:

CVE	Title	Impact on
CVE-2022-2825	STACK-BASED BUFFER OVERFLOW CWE-121	Marine ITMonitoring 1.0.2, 1.0.3

© Copyright 2022 ABB. All rights reserved.

CVE	Title	Impact on
CVE-2022-2848	HEAP-BASED BUFFER OVERFLOW CWE-122	Marine ITMonitoring 1.0.2, 1.0.3

Recommended immediate actions

ABB advises affected customers to contact ABB Marine Support to install the below mentioned KEPServerEX update to address the mentioned vulnerabilities in KEPServerEX. Also, it is advised to review the Mitigating factors and Workarounds sections for additional advice on how to reduce the risk associated with this vulnerability.

PTC recommended KEPServerEX software update:

- Kepware KEPServerEX should upgrade to v6.12 or later

ABB recommends that customers apply the update at earliest convenience.

Vulnerability severity and details

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

CVE-2022-2825 and STACK-BASED BUFFER OVERFLOW CWE-121

CVSS v3.1 Base Score:	9.8 (High)
CVSS v3.1 Vector:	CVSS:3.1/ AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
NVD Summary Link:	http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-2825

CVE-2022-2848 and HEAP-BASED BUFFER OVERFLOW CWE-122

CVSS v3.1 Base Score:	9.1 (High)
CVSS v3.1 Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H
NVD Summary Link:	http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-2848

Mitigating factors

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

© Copyright 2022 ABB. All rights reserved.

Workarounds

PTC has tested the following workaround, which consist in turning off the OPC UA interface. Although such workaround will not correct the underlying vulnerability, it can help block the known attack vectors.

PTC also advises with the workaround to turn off the OPC UA interface from KEPServerEX Configuration utility.

It is important to note that the OPC UA interface is ON by default after installing the KEPServerEX software in the system.

Perform the following actions in the KEPServerEX configuration utility to turn off the OPC UA interface:

1. Right click the Project folder in the project tree
2. Select Properties
3. Select OPC UA
4. Under Server Interface toggle Enable to Off
5. Click Apply

For additional instructions and support please contact Global Marine Support: support.marine@abb.com.

Frequently asked questions

What is the scope of the vulnerability?

Exploiting these vulnerabilities using the specially crafted OPC UA messages could crash the server and leak data transmitted to that server.

What causes the vulnerability?

The vulnerability in the Marine product is cause by a buffer overflow vulnerability in the OPC UA stack of KEPServerEX, a component of the Marine ITMonitoring product.

What is KEPServerEX?

KEPServerEX is the connectivity platform that allows users can connect, manage, monitor, and control diverse automation devices and software applications through one intuitive user interface. KEPServerEX leverages OPC and IT-centric communication protocols (such as SNMP, ODBC, and web services) to provide users with a single source for industrial data.

This connectivity platform is used in Marine ITMonitoring version 1.0.2 and 1.0.3.

What might an attacker use the vulnerability to do?

Exploiting these vulnerabilities using the specially crafted OPC UA messages could crash the server and leak data transmitted to that server and loss of connectivity.

© Copyright 2022 ABB. All rights reserved.

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?

No. Functional safety is not affected.

What does the update do?

KEPServerEX version 6.12 and later are not affected by the mentioned vulnerabilities.

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

Yes, the PT KEPServerEX vulnerabilities have been publicly disclosed.

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.

© Copyright 2022 ABB. All rights reserved.

References

Article CS375312	Security vulnerability identified in PTC Kepware Products

Support

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

Global Marine Support: support.marine@abb.com

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	2023-01-02

© Copyright 2022 ABB. All rights reserved.