DOCUMENT ID: 2CMT006086
REVISION: A
DATE: 2022-05-26

CYBER SECURITY ADVISORY

SECURITY - e-Design - Multiple vulnerabilities

CVE-2022-28702, CVE-2022-29483

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

e-Design, all versions up to and including 1.12.2.0004

Vulnerability IDs

CVE-2022-28702, CVE-2022-29483

Summary

ABB is aware of public reports of two vulnerabilities in the product versions listed above. An update is available that resolves the privately reported vulnerabilities in the product versions listed above.

An attacker who successfully exploited these vulnerabilities could:

a) create a DoS condition on the target machine (on which e-Design is installed) after a reboot.

b) achieve SYSTEM user permissions on target machine after privilege escalation from local low privileged user.

Recommended immediate actions

The problem is corrected in the following product version: e-Design 1.12.2.0006

It can be downloaded on: https://search.abb.com/library/Download.aspx?DocumentID=9AKK106103A3346

ABB recommends that customers apply the update at earliest convenience.

Vulnerability severity and details

Multiple vulnerabilities exist in the product versions listed above. The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) v3.1[1].

The vulnerabilities are caused by improper folder permissions set during installation of e-Design.

CVE-2022-28702: ABB e-Design Link Following Denial-of-Service Vulnerability

CVSS v3.1 Base Score:	6.1 (Medium)
CVSS v3.1 Temporal Score:	5.5 (Medium)
CVSS v3.1 Vector:	CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H/E:P/RL:O/RC:C
NVD Summary Link:	https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H/E:P/RL:O/RC:C

CVE-2022-29483: ABB e-Design Link Following Local Privilege Escalation Vulnerability

A local low privileged attacker to create a DoS condition on the target machine after a reboot.

CVSS v3.1 Base Score:	7.8 (High)
CVSS v3.1 Temporal Score:	7.0 (High)
CVSS v3.1 Vector:	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
NVD Summary Link:	https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

Mitigating factors

Since the vulnerabilities can be exploited only by physically accessing the target machine on which e-Design is installed, the owner of the machine should not let any other user login until the fix is applied. Machine owner should not leave the machine unlocked when away.

Workarounds

No workaround exists. Refer to the chapter mitigating factors to limit the exposure for the vulnerabilities.

[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.

Frequently asked questions

What is the scope of the vulnerabilities?

An attacker who successfully exploited these vulnerabilities could cause:

a) DoS condition on the target machine, preventing the target machine to startup properly after reboot.

b) local low privileged user to elevate privileges to SYSTEM on the target machine.

What causes the vulnerability?

The issue is caused by a combination of MSI installer behavior and symbolic links created in folders with admin rights.

What is e-Design?

e-Design is the single point of access to ABB Electrification Design Software tools.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited these vulnerabilities could install malicious software executing with SYSTEM permissions violating confidentiality, integrity, and availability of the target machine.

How could an attacker exploit the vulnerability?

An attacker could try to exploit these vulnerabilities by crafting specific files on the target machine causing either DoS of the target machine or local user privilege escalation to SYSTEM user. This would require that attacker has physical access to the machine and that the machine is unlocked.

Could the vulnerability be exploited remotely?

No.

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

No. Only the local machine can be compromised.

What does the update do?

The update fixes the folder permissions created at installation time.

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.

More information on recommended practices can be found in the following documents:

Acknowledgement

ABB thanks the Trend Micro's Zero Day Initiative (ZDI), more specifically Michael DePlante (@izobashi) for helping to identify the vulnerability and protecting our customers.

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	2022-05-26