DOCUMENT ID: 9AKK108466A8261
REVISION: B
DATE: 2022-07-26

CYBER SECURITY NOTIFICATION

Cyber Security Notification – Industroyer2

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.

Purpose

ABB has a rigorous cyber security program which involves not only internal processes to ensure product security but also external engagement with the wider cybersecurity community and 3rd party suppliers. Occasionally an issue is identified with the potential to impact ABB products and systems.

Generally, this means 3rd party product vulnerabilities or life-cycle issues to which ABB products may have a dependency on. Another example could be threats which are not directly targeting ABB products however may constitute a threat to environments where ABB products/systems operate.

When a potential threat is identified or reported, ABB immediately initiates our vulnerability handling process. This entails an evaluation to determine if there are steps which can be taken to reduce risk and maintain functionality for the end user.

The result may be the publication of a Cyber Security Notification. This intends to notify customers of the issue 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 Notification should not be assumed as an 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 Notification is an example of ABB's commitment to the user community in support of this critical topic. The release of a Notification intends to provide timely information which is essential to help ensure our customers are fully informed. See details below and refer to the section on "General security recommendations" for further advise on how to keep your systems secure.

Background

On 2022-04-12, the discovery of a malware framework called Industroyer2 (sometimes also referred to as Industroyer.V2) was made public. This malware framework reportedly simplifies attacks against certain types of industrial control systems and specifically certain devices within such systems. With this framework, a successful exploit could allow attackers to change outputs of affected devices. Exploiting these vulnerabilities requires that the attacker can establish an initial access to the target network.

Potentially affected products

The framework reportedly leverages technologies such as IEC 60870-5-104 (IEC-104) which are widely used in many Industrial Control Systems. Products using a pre-configured scheme for IEC 60870-5- 104 (IEC 104) information object addresses will enable a generic exploit against switching objects by the malware, provided that the attacker has succeeded in deploying the malware in the OT system. These ABB relays have a documented preconfigured set of IEC 60870-5-104 (IEC-104) objects and thus could become a target of such an attack:

- ABB REC/RER615 protection relays
- ABB RER620 protection relays

Mitigating factors

Since the Industroyer2 framework utilizes functionalities in the targeted devices and interfaces, which are otherwise used by legitimate users and in legitimate use cases, mitigating factors are primarily about reducing the external attack surface to a minimum, e.g. by segregating the network and isolating to the degree possible and by disabling functionalities and network services.

Recommended immediate actions

- Verify if the IEC 60870-5-104 (IEC 104) client's (i.e., controlling entity's) IP address is configured in the relay. If not, consider changing the default wildcard address 0.0.0.0 to the IP address of the controlling entity. This will exclude other clients from accessing the relay.
- Consider re-arranging the default IEC 60870-5-104 (IEC 104) object addresses into non-defaults.

Vulnerability Details

See links below for more details.

- CERT-UA : https://cert.gov.ua/article/39518
- ESET: https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/

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.

References

Further information

ESET	https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-re-loaded/
CERT-UA	https://cert.gov.ua/article/39518

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/cyber-security.

Revision history

Rev. Ind.	Page (p) Chapter (c)	Change description	Rev. date
A	all	Initial version	2022-04-26
B	all	Additional information added	2022-07-26