DOCUMENT ID: 7PAA013309
REVISION: B
DATE: 2024-06-14
SECURITY LEVEL: PUBLIC

CYBER SECURITY ADVISORY

System 800xA
SECURITY Advisory - ABB 800xA Base 6.0.x, 6.1.x CSLib communication DoS vulnerability

CVE ID: CVE-2024-3036

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 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 (e.g. ICS-CERT).

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

ABB 800xA Base	versions 6.1.1-2 and earlier

Vulnerability IDs and Product Issue Numbers (PIN)

CVE-2024-3036, PIN-H2JU3T

Summary

ABB is aware of a vulnerability in the product versions listed above.

An attacker who successfully exploited this vulnerability could cause services to crash and restart by sending specifically crafted messages.

The vulnerability only affects 800xA services in PC based client/server nodes. Controllers are not affected by this vulnerability.

Recommended immediate actions

The problem is or will be corrected in the following product versions:

- ABB 800xA Base 6.2.0-0 (part of System 800xA 6.2.0.0)
- ABB 800xA Base 6.1.1-3 (part of System 800xA 6.1.1.2)
- ABB 800xA Base 6.0.3-x (included in next revision)

It is recommended to update to an active product version to obtain the latest corrections.

Vulnerability severity and details

A vulnerability exists in the product versions listed above. An attacker who successfully exploited this vulnerability could cause services to crash by sending specifically crafted messages.

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) for both v3.1[1] and v4.0[2].

CVE-2024-3036: Communication DoS vulnerability

An attacker who successfully exploited this vulnerability could cause services to crash by sending specifically crafted messages.

CVSS v3.1 Base Score:	5.7
CVSS v3.1 Temporal Score:	5.1
CVSS v3.1 Vector:	CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CVSS v4.0 Score	6.9
CVSS v4.0 Vector:	CVSS:4.0/AV:A/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/S:N/AU:Y/R:A/V:D/RE:M
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2024-3036

Mitigating factors

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

[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.

[2] For the CVSS v4.0 scoring only the CVSS Base Metrics and the CVSS Supplemental Metrics (if information is available) are considered in this advisory. The CVSS Environmental and Threat Metrics, which can affect the vulnerability severity, are not provided in this advisory since they reflect the potential impact of a vulnerability within the end-user organizations’ computing environment and over time depending on the vulnerability exploit maturity. Therefore, end-user organizations are recommended to analyze their situation and specify the Environmental and Threat Metrics.

Workarounds

The system can be protected from network-based exploits of this vulnerability by enabling IPSec according to existing user documentation (See References).

Frequently asked questions

What is the scope of the vulnerability?

An attacker who successfully exploited this vulnerability could, by using a malicious application that connects to a server application (applicable for all 800xA Base server applications), cause the server to crash by sending some specifically crafted message.

What causes the vulnerability?

The vulnerability is caused by an unchecked buffer.

What is 800xA Base?

800xA Base is the core platform for System 800xA that consists of both core service applications for basic Workplace operations as well as a framework for other System 800xA products.

What is CSLib?

CSLib is a TCP/IP based protocol that is commonly used by 800xA clients and services.

What might an attacker use the vulnerability to do?

Denial of service. An attacker can create denial of services by continuously sending special crafted messages to the service in the system. The impacted service will be automatically restarted. For a redundant system using failover functionality there will be a failover to the redundant service, which may also be impacted by such an attack, stopping the affected service. The services will be attempted to be restarted by the System. However, if the attack is persistent, they will not be able to overcome this.

Note that repeated restarts of the affected service could be an indication of a compromise.

How could an attacker exploit the vulnerability?

If the attacker has access to the Client/Server network and IPSec is not enabled the attacker can connect to the server applications using TCP/IP sockets and send specially crafted messages to exploit this.

The vulnerability only affects 800xA services in PC based client/server nodes. Controllers are not affected by this vulnerability.

Could the vulnerability be exploited remotely?

If IPSec is not enabled there is a possibility to exploit remotely.

If IPSec is enabled the attacker would first need physical access to the system and plant a trojan or similar in a system node.

What does the update do?

The unchecked buffer is now managed and checked in a secure way.

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

Control systems and the control network are exposed to cyber threats. In order to minimize these risks, the protective measures and best practices listed below are available in addition to other measures. ABB strongly recommends system integrators and asset owners to implement the measures they consider appropriate for their control system environment:

- Place control systems in a dedicated control network containing control systems only.
- Locate control networks and systems behind firewalls and separate them from any other networks like business networks and the Internet.
- Block any inbound Internet traffic destined for the control networks/systems. Place remote access systems used for remote control system access outside the control network.
- Limit outbound Internet traffic originating from control systems/networks as much as possible. If control systems must talk to the Internet, tailor firewall rules to required resources - allow only source IPs, destination IPs and services/destination ports which control systems definitely need to use for normal control operation.
- If Internet access is required on occasion only, disable relevant firewall rules and enable them during the time window of required Internet access only. If supported by your firewall, define an expiry date and time for such rules – after the expiry date and time, the firewall will disable the rule automatically.
- Limit exposure of control networks/systems to internal systems. Tailor firewall rules allowing traffic from internal systems to control networks/systems to allow only source IPs, destination IPs and services/destination ports which are definitely required for normal control operation.
- Create strict firewall rules to filter malicious network traffic targeting control system vulnerabilities ("exploit traffic"). Exploit traffic may use network communication features like source routing, IP fragmentation and/or IP tunneling. If such features are not required for normal control operation, block them on your firewall.
- If supported by your firewall, apply additional filters to allowed traffic which provide protection for control networks/systems. Such filters are provided by advanced firewall features like Application Control and Anti-Virus.
- Use Intrusion Detection Systems (IDS) or Intrusion Preventions Systems (IPS) to detect/block control system-specific exploit traffic. Consider using IPS rules protecting against control system exploits.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs). Please ensure that VPN solutions are updated to the most current version available.
- In case you want to filter internal control network traffic, consider using solutions supporting Intra-LAN traffic control like VLAN access control lists.
- Harden your control systems by enabling only the ports, services and software required for normal control operation. Disable all other ports and disable/uninstall all other services and software.
- If possible, limit the permissions of user accounts, software processes and devices to the permissions required for normal control operation.
- Use trusted, patched software and malware protection solutions. Interact with trusted web sites and trusted email attachments only.
- 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.

– Protect control systems from physical access by unauthorized personnel e.g. by placing them in locked switch cabinets.

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

3BSE034463-611 System 800xA 6.1.1 Reference – Network Configuration

Acknowledgement

ABB acknowledges and extends gratitude to Uri Sade, Roman Dvorkin, Roni Gavrilov, and Eran Jacob of the OTORIO org for responsibly disclosing the vulnerability and providing valuable input on product improvements.

References

Refer below document for information about how to setup IPSec configuration.

2PAA111693-611 System 800xA 6.1.1 Installation, Update and Upgrade - Post Installation

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 https://global.abb/group/en/technology/cyber-security.

Revision history

Rev. Ind.	Page (p) Chapter (c)	Change description	Rev. date
A	all	Initial version	2024-06-05
B	P3	Included CVSS v4.0 score.	2024-06-14