DOCUMENT ID: 7PAA012159
REVISION: B
DATE: 2025-01-31
SECURITY LEVEL: PUBLIC

CYBER SECURITY ADVISORY

System 800xA
SECURITY Advisory - System 800xA 5.1.x, 6.0.3.x, 6.1.1.x, 6.2.x - VideONet Camera passwords stored in clear text

CVE ID: CVE-2024-10334

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 (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

The following product versions that use VideONet are affected by this issue. Please note that no updates will be available to correct the issue. Instead, a transition to the new product Camera Connect will be offered. For more information, see further below.

- System 800xA 5.1.x
- System 800xA 6.0.3.x
- System 800xA 6.1.1.x
- System 800xA 6.2.x

Vulnerability IDs and Product Issue Numbers (PIN)

CVE ID	Product Issue Number*
CVE-2024-10334	PIN-5B87TA

* Product Issue Number – is an ABB internal unique identifier to identify an issue. The Product Issue Number is for example used to identify the correction of an issue in Release Notes.

Summary

ABB is aware of a vulnerability related to the VideONet product. The vulnerabilitiy is applicable in the System 800xA versions listed above, where the VideONet product is used. There will be no update/resolution of this vulnerability in System 800xA. Instead, the strategy for ABB is to offer existing customers using VideONet a transfer to a new product, Camera Connect. This will be offered as soon as Camera Connect is available as a product.

An attacker who successfully exploited the vulnerability could, in the worst case scenario, stop or manipulate the video feed.

There is no impact to other Operator station functions (graphics, trends, faceplates, etc) and Control operations are not impacted at all.

Recommended immediate actions

ABB recommends following the guidelines described in the *System 800xA VideONet Connect user documentation (2PAA109407*)*. The user documentation explains how to protect the network on which cameras are connected from unauthorized access and the recommended deployment. Similarly, it is important to protect the VideONet Server from unauthorized access.

There will be no update for VideONet in System 800xA. Instead, the recommendation is to transfer to the new product, Camera Connect, as soon as it becomes available. Camera Connect is expected to be released in the first half of 2025. Customers may proactively reach out to their ABB contact in case they would like to receive further information about the new Camera Connect solution.

Ensure that the camera user accounts used by System 800xA only have the minimum level of permission needed to perform the required task, e.g. do not use an administrator or superuser account. This limits the potential damage from a leaked password.

Vulnerability severity and details

A vulnerability exists in the VideONet product included in the listed System 800xA versions, where VideONet is used.

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) 4.0[1].

CVE-2024-10334 Camera passwords stored in clear text

An attacker who successfully exploited this vulnerability could retrieve the login credentials for all cameras and manipulate or stop the video feed.

CVSS

CVSS v3.1 Base Score:	7.3
CVSS v3.1 Temporal Score:	6.2
CVSS v3.1 Vector:	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:H/E:U/RL:U/RC:U
CVSS v4.0 Score	7.0
CVSS v4.0 Vector:	CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:L/VA:H/SC:N/SI:N/SA:N/S:N/AU:N/R:U/V:D/RE:M

CWE

CWE-256:	Plaintext Storage of a Password

CVE

NVD Summary Link:	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-10334

Mitigating factors

Follow the guidelines in the *System 800xA VideONet Connect user documentation (2PAA109407*)* to secure and protect the installation of, and the network where VideONet is running.

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

Workarounds

The only possible workaround is to secure and protect the network where VideONet is running and the VideONet Server from unauthorized access.

The workaround will not correct the underlying vulnerability, but it helps blocking known attack vectors. 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.

Frequently asked questions

What is the scope of the vulnerability?

An attacker who successfully exploited this vulnerability could retrieve the login credentials for all cameras and could, in the worst case scenario, stop or manipulate the video feed.

What causes the vulnerability?

The vulnerability is caused by the passwords for the cameras being stored in clear text in the database which is available in all clients running VideONet.

What is VideONet?

VideONet is used for video/camera surveillance as a part of the Distributed Control System (DCS).

What might an attacker use the vulnerability to do?

An attacker who successfully exploited the vulnerability could retrieve the login credentials for all cameras. In the worst case scenario, the attacker could stop or manipulate the video feed.

How could an attacker exploit the vulnerability?

The attacker could locate the configuration where the passwords are stored.

To exploit the vulnerability it would require that the attacker has access to the system network, by connecting to the network either directly or through a wrongly configured or penetrated firewall, or installs 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?

If IPSec is not enabled there is a possibility to exploit this vulnerability 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?

There will not be any update of the VideONet product. The strategy for ABB is to abandon VideONet and instead offer a new product, Camera Connect. This is valid both for new customers and for existing customers using VideONet, where a transfer from VideONet to Camera Connect will be offered.

This will be done as soon as Camera Connect is available.

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

No.

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 the 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 ("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:

3BSE034463D6200 System 800xA 6.2 Reference – Network Configuration

References

2PAA109407D6200 System 800xA 6.2 Operations – VideONet Connect

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
B	all	Initial version There were some minor issues detected after approval of Rev A which needed to be updated, and therefor we created a Rev B. Revision A was never published.	2025-01-13