
CYBER SECURITY ADVISORY

System 800xA affected by 3rd party component vulnerabilities

Vulnerability ID: CVE-2025-55188, CVE-2025-53817, CVE-2025-53816, CVE-2025-11002, CVE-2025-11001, CVE-2025-0411, CVE-2024-11612, CVE-2024-11477, CVE-2023-52169, CVE-2023-52168, CVE-2023-40481, CVE-2023-31102, CVE-2022-47112, CVE-2022-47111, CVE-2022-29072, CVE-2024-26203
Product Issue Numbers (PIN) : PIN-V1UM0J- 7-Zip Vulnerability, PIN-GP2LE7- Azure Data Studio Vulnerability.

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

ABB 800xA History	versions 7.0 and earlier
ABB Batch Management	versions 6.2 and earlier
ABB Production Response Batch History	versions 6.2 and earlier
ABB 800xA for Symphony Plus Harmony	versions 6.2 and earlier
ABB 800xA for AC 870P Melody	versions 6.2 and earlier
ABB Application Change Management	versions 6.2 and earlier

Vulnerability IDs and Product Issue Numbers (PIN)

CVE-2025-55188, CVE-2025-53817, CVE-2025-53816, CVE-2025-11002, CVE-2025-11001, CVE-2025-0411, CVE-2024-11612, CVE-2024-11477, CVE-2023-52169, CVE-2023-52168, CVE-2023-40481, CVE-2023-31102, CVE-2022-47112, CVE-2022-47111, CVE-2022-29072, CVE-2024-26203 Product Issue Numbers (PIN) : PIN-V1UM0J- 7-Zip Vulnerability, PIN-GP2LE7- Azure Data Studio Vulnerability.

Summary

ABB is aware of public reports of vulnerabilities in 7-Zip version 18.5 and Microsoft Azure Data Studio version 1.32 included in the product versions listed above.

CVE	Title	Impacted 800xA Product
CVE-2025-55188	7-Zip before 25.01 Improper Symbolic Link Handling Vulnerability During Extraction	ABB 800xA History

CVE-2025-53817	7-Zip a null pointer dereference in the Compound handler may lead to denial of service.	ABB 800xA History
CVE-2025-53816	7-Zip Zeroes written outside heap buffer in RAR5 handler may lead to memory corruption and denial of service in versions	ABB 800xA History
CVE-2025-11002	7-Zip ZIP File Parsing Directory Traversal Remote Code Execution Vulnerability	ABB 800xA History
CVE-2025-11001	7-Zip ZIP File Parsing Directory Traversal Remote Code Execution Vulnerability	ABB 800xA History
CVE-2025-0411	7-Zip Mark-of-the-Web Bypass Vulnerability	ABB 800xA History
CVE-2024-11612	7-Zip CopyCoder Infinite Loop Denial-of-Service Vulnerability	ABB 800xA History
CVE-2024-11477	7-Zip Zstandard Decompression Integer Underflow Remote Code Execution Vulnerability	ABB 800xA History
CVE-2023-52169	7-Zip Information Disclosure Vulnerability	ABB 800xA History
CVE-2023-52168	7-Zip NTFS Handler Buffer Overflow Flaw	ABB 800xA History
CVE-2023-40481	7-Zip SquashFS File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability.	ABB 800xA History
CVE-2023-31102	7-Zip Buffer Overflow Vulnerability	ABB 800xA History
CVE-2022-47112	7-Zip vulnerability does not report an error for certain invalid xz files	ABB 800xA History
CVE-2022-47111	7-Zip 22.01 does not report an error for certain invalid xz files	ABB 800xA History
CVE-2022-29072	7-Zip for Windows Heap Overflow via Drag-and-Drop to Help Contents Allows Command Execution	ABB 800xA History
CVE-2024-26203	Azure Data Studio Elevation of Privilege Vulnerability	ABB Batch Management, ABB Production Response Batch History, ABB 800xA for Symphony Plus Harmony, ABB 800xA for AC 870P Melody, ABB Application Change Management

The vulnerability in 7-Zip can be exploited if attacker gains control over the system and extracts a malicious file using this version of 7-Zip. Otherwise, the attacker must force the user to visit malicious websites or click links and extract the package through 7-zip.

Microsoft Azure Data Studio gets installed along with SQL Server Management Studio. An attacker who successfully exploits vulnerability in Microsoft Azure Data studio may compromise the security of the product by gaining privileges, reading sensitive information, executing commands, evading detection, etc. if the Authentication, Authorization and Accountability is not configured properly in the system.

However, none of the products listed above uses Microsoft Azure Data Studio. Microsoft Azure Data Studio is automatically removed from the system from System 800xA 7.0 onwards.

These vulnerabilities may appear when the product media is scanned. However, they can only be exploited if the vulnerable software is installed on the system. For this reason, it is strongly advised to uninstall outdated or vulnerable versions of third-party software immediately.

Recommended immediate actions

ABB recommends uninstalling the version of 7-Zip and Microsoft Azure Data Studio from the system. Uninstallation does not affect the functionality of the products.

ABB recommends that customers perform the uninstallation at earliest convenience.

Vulnerability severity and details

A vulnerability exists in the 7-Zip and Microsoft Azure Data Studio included in the 800xA product versions listed above. The presence of these two third party software does not affect the functionality or working of the 800xA products. It can safely be uninstalled. The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS)¹ for both v3.1² and v4.0³.

The indicated Common Weakness Enumerations (CWE) have been selected from the MITRE CWE list⁴.

CVE-2025-55188 – 7-Zip Vulnerability

7-Zip before does not always properly handle symbolic links during extraction.

CVSS

CVSS v3.1 Base Score: 3.6 (Low)

CVSS v3.1 Temporal Score: 3.3 (Low)

CVSS v3.1 Vector: **CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N/E:P/RL:O/RC:C**

CVSS v4.0 Score: NVD assessment not yet provided.

CVSS v4.0 Vector: NVD assessment not yet provided.

CWE

CWE-59: Improper Link Resolution Before File Access ('Link Following')

¹ Common Vulnerability Scoring System (CVSS), Forum of Incident Response and Security Teams, Inc., <https://www.first.org/cvss/>.

² For the CVSS v3.1 scoring only the CVSS Base Score and the Temporal Score (if information is available) are considered in this advisory. 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.

³ 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.

⁴ Common Weakness Enumeration (CWE), The MITRE Corporation, <https://cwe.mitre.org/>.

CVE

NVD Summary Link: [NVD - CVE-2025-55188](https://nvd.nist.gov/vuln/detail/CVE-2025-55188) (https://nvd.nist.gov/vuln/detail/CVE-2025-55188)

CVE-2025-53817 – 7-Zip Vulnerability

7-Zip is a file archiver with a high compression ratio. 7-Zip supports extracting from Compound Documents.

CVSS

CVSS v3.1 Base Score: 7.5 (High)

CVSS v3.1 Temporal Score: 6.7 (Medium)

CVSS v3.1 Vector: **CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C**

CVSS v4.0 Score: 5.5 (Medium)

CVSS v4.0 Vector: **CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:P**

CWE

CWE-476: NULL Pointer Dereference

CVE

NVD Summary Link: [NVD - CVE-2025-53817](https://nvd.nist.gov/vuln/detail/CVE-2025-53817) (https://nvd.nist.gov/vuln/detail/CVE-2025-53817)

CVE-2025-53816 – 7-Zip Vulnerability

7-Zip is a file archiver with a high compression ratio. Zeroes written outside heap buffer in RAR5 handler may lead to memory corruption and denial of service in versions of 7-Zip.

CVSS

CVSS v3.1 Base Score: 7.5 (High)

CVSS v3.1 Temporal Score: 6.5 (Medium)

CVSS v3.1 Vector: **CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C**

CVSS v4.0 Score: 5.5 Medium

CVSS v4.0 Vector: **CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:P**

CWE

CWE-122: Heap-based Buffer Overflow

CVE

NVD Summary Link: [NVD - CVE-2025-53816](https://nvd.nist.gov/vuln/detail/CVE-2025-53816) (https://nvd.nist.gov/vuln/detail/CVE-2025-53816)

CVE-2025-11002 - 7-Zip ZIP File Parsing Directory Traversal Remote Code Execution Vulnerability

This vulnerability allows remote attackers to execute arbitrary code on affected installations of 7-Zip. Crafted data in a ZIP file can cause the process to traverse to unintended directories.

CVSS

CVSS v3.1 Base Score: 7.0 (High)

CVSS v3.1 Temporal Score: 6.1 (Medium)

CVSS v3.1 Vector: **CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C**

CVSS v4.0 Score: NVD assessment not yet provided.

CVSS v4.0 Vector: NVD assessment not yet provided.

CWE

CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

CVE

NVD Summary Link: [NVD - CVE-2025-11002](https://nvd.nist.gov/vuln/detail/CVE-2025-11002) (https://nvd.nist.gov/vuln/detail/CVE-2025-11002)

CVE-2025-11001 - 7-Zip ZIP File Parsing Directory Traversal Remote Code Execution Vulnerability

This vulnerability allows remote attackers to execute arbitrary code on affected installations of 7-Zip. Crafted data in a ZIP file can cause the process to traverse to unintended directories.

CVSS

CVSS v3.1 Base Score: 7.8 (High)

CVSS v3.1 Temporal Score: 6.8 (Medium)

CVSS v3.1 Vector: **CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C**

CVSS v4.0 Score: NVD assessment not yet provided.

CVSS v4.0 Vector: NVD assessment not yet provided.

CWE

CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

CVE

NVD Summary Link: [NVD - CVE-2025-11001](https://nvd.nist.gov/vuln/detail/CVE-2025-11001) (https://nvd.nist.gov/vuln/detail/CVE-2025-11001)

CVE-2025-0411 - 7-Zip Mark-of-the-Web Bypass Vulnerability

This vulnerability allows remote attackers to bypass the Mark-of-the-Web protection mechanism on affected installations of 7-Zip. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.

CVSS

CVSS v3.1 Base Score: 7.0 (High)

CVSS v3.1 Temporal Score: 6.5 (Medium)

CVSS v3.1 Vector: **CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C**

CVSS v4.0 Score: NVD assessment not yet provided.

CVSS v4.0 Vector: NVD assessment not yet provided.

CWE

CWE-693: Protection Mechanism Failure

CVE

NVD Summary Link: [NVD - CVE-2025-0411](https://nvd.nist.gov/vuln/detail/CVE-2025-0411) (https://nvd.nist.gov/vuln/detail/CVE-2025-0411)

CVE-2024-11612 - 7-Zip CopyCoder Infinite Loop Denial-of-Service Vulnerability

This vulnerability allows remote attackers to create a denial-of-service condition on affected installations of 7-Zip.

CVSS

CVSS v3.1 Base Score: 6.5 (Medium)

CVSS v3.1 Temporal Score: 5.7 (Medium)

CVSS v3.1 Vector: **CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C**

DOCUMENT ID: 7PAA023732
REVISION: A
DATE: 2026-03-31

SYSTEM 800XA AFFECTED BY 3RD PARTY COMPONENT VULNERABILITIES

CVSS v4.0 Score: NVD assessment not yet provided.
CVSS v4.0 Vector: NVD assessment not yet provided.

CWE

CWE-835: Loop with Unreachable Exit Condition ('Infinite Loop')

CVE

NVD Summary Link: [NVD - CVE-2024-11612](https://nvd.nist.gov/vuln/detail/CVE-2024-11612) (https://nvd.nist.gov/vuln/detail/CVE-2024-11612)

CVE-2024-11477 - 7-Zip Zstandard Decompression Integer Underflow Remote Code Execution Vulnerability.

This vulnerability allows remote attackers to execute arbitrary code on affected installations of 7-Zip. Interaction with this library is required to exploit this vulnerability

CVSS

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:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C**

CVSS v4.0 Score: NVD assessment not yet provided.
CVSS v4.0 Vector: NVD assessment not yet provided.

CWE

CWE-191: Integer Underflow (Wrap or Wraparound)

CVE

NVD Summary Link: [NVD - CVE-2024-11477](https://nvd.nist.gov/vuln/detail/CVE-2024-11477) (https://nvd.nist.gov/vuln/detail/CVE-2024-11477)

CVE-2023-52169 – 7-Zip Vulnerability

The NtfsHandler.cpp NTFS handler in 7-Zip before 24.01 (for 7zz) contains an out-of-bounds read that allows an attacker to read beyond the intended buffer. The bytes read beyond the intended buffer are presented as a part of a filename listed in the file system image

CVSS

CVSS v3.1 Base Score: 8.2 (High)
CVSS v3.1 Temporal Score: 7.1 (High)
CVSS v3.1 Vector: **CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H/E:U/RL:O/RC:C**

CVSS v4.0 Score: NVD assessment not yet provided.
CVSS v4.0 Vector: NVD assessment not yet provided.

CWE

CWE-125: Out-of-bounds Read

CVE

NVD Summary Link: [NVD - CVE-2023-52169](https://nvd.nist.gov/vuln/detail/CVE-2023-52169) (https://nvd.nist.gov/vuln/detail/CVE-2023-52169)

CVE-2023-52168 – 7-Zip Vulnerability

The NtfsHandler.cpp NTFS handler in 7-Zip before 24.01 (for 7zz) contains a heap-based buffer overflow that allows an attacker to overwrite two bytes at multiple offsets beyond the allocated buffer size: $\text{buffer} + 512 * i - 2$, for $i = 9, i = 10, i = 11$, etc.

CVSS

CVSS v3.1 Base Score: 8.4 (High)
CVSS v3.1 Temporal Score: 7.3 (High)
CVSS v3.1 Vector: **CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C**

CVSS v4.0 Score: NVD assessment not yet provided.
CVSS v4.0 Vector: NVD assessment not yet provided.

CWE

CWE-122: Heap-based Buffer Overflow

CVE

NVD Summary Link: **NVD - CVE-2023-52168** (<https://nvd.nist.gov/vuln/detail/CVE-2023-52168>)

CVE-2023-40481 - 7-Zip SquashFS File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability.

This vulnerability allows remote attackers to execute arbitrary code on affected installations of 7-Zip. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.

CVSS

CVSS v3.1 Base Score: 7.8 (High)
CVSS v3.1 Temporal Score: 6.8 (Medium)
CVSS v3.1 Vector: **CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C**

CVSS v4.0 Score: NVD assessment not yet provided.
CVSS v4.0 Vector: NVD assessment not yet provided.

CWE

CWE-787: Out-of-bounds Write

CVE

NVD Summary Link: **NVD - CVE-2023-40481** (<https://nvd.nist.gov/vuln/detail/CVE-2023-40481>)

CVE-2023-31102 – 7-Zip vulnerability

Ppmd7.c in 7-Zip before 23.00 allows an integer underflow and invalid read operation via a crafted 7Z archive.

CVSS

CVSS v3.1 Base Score: 7.8 (High)
CVSS v3.1 Temporal Score: 6.8 (Medium)
CVSS v3.1 Vector: **CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C**

CVSS v4.0 Score: NVD assessment not yet provided.
CVSS v4.0 Vector: NVD assessment not yet provided.

DOCUMENT ID: 7PAA023732
REVISION: A
DATE: 2026-03-31

SYSTEM 800XA AFFECTED BY 3RD PARTY COMPONENT VULNERABILITIES

CWE

CWE-191: Integer Underflow (Wrap or Wraparound)

CVE

NVD Summary Link: [NVD - CVE-2023-31102](https://nvd.nist.gov/vuln/detail/CVE-2023-31102) (https://nvd.nist.gov/vuln/detail/CVE-2023-31102)

CVE-2022-47112 – 7-Zip vulnerability

7-Zip does not report an error for certain invalid xz files, involving stream flags and reserved bits.

CVSS

CVSS v3.1 Base Score: 3.3 (Low)

CVSS v3.1 Temporal Score: 3.2 (Low)

CVSS v3.1 Vector: **CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:U/RC:C**

CVSS v4.0 Score: NVD assessment not yet provided.

CVSS v4.0 Vector: NVD assessment not yet provided.

CWE

CWE-754: Improper Check for Unusual or Exceptional Conditions

CVE

NVD Summary Link: [NVD - CVE-2022-47112](https://nvd.nist.gov/vuln/detail/CVE-2022-47112) (https://nvd.nist.gov/vuln/detail/CVE-2022-47112)

CVE-2022-47111 – 7-Zip vulnerability

7-Zip 22.01 does not report an error for certain invalid xz files, involving block flags and reserved bits. Some later versions are unaffected.

CVSS

CVSS v3.1 Base Score: 3.3 (Low)

CVSS v3.1 Temporal Score: 3.2 (Low)

CVSS v3.1 Vector: **CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:U/RC:C**

CVSS v4.0 Score: NVD assessment not yet provided.

CVSS v4.0 Vector: NVD assessment not yet provided.

CWE

CWE-754: Improper Check for Unusual or Exceptional Conditions

CVE

NVD Summary Link: [NVD - CVE-2022-47112](https://nvd.nist.gov/vuln/detail/CVE-2022-47112) (https://nvd.nist.gov/vuln/detail/CVE-2022-47112)

CVE-2022-47111 – 7-Zip vulnerability

7-Zip 22.01 does not report an error for certain invalid xz files, involving block flags and reserved bits. Some later versions are unaffected.

CVSS

CVSS v3.1 Base Score: 3.3 (Low)

CVSS v3.1 Temporal Score: 3.2 (Low)

CVSS v3.1 Vector: **CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:U/RC:C**

DOCUMENT ID: 7PAA023732
REVISION: A
DATE: 2026-03-31

SYSTEM 800XA AFFECTED BY 3RD PARTY COMPONENT VULNERABILITIES

CVSS v4.0 Score: NVD assessment not yet provided.
CVSS v4.0 Vector: NVD assessment not yet provided.

CWE

CWE-754: Improper Check for Unusual or Exceptional Conditions

CVE

NVD Summary Link: [NVD - CVE-2022-47112](https://nvd.nist.gov/vuln/detail/CVE-2022-47112) (https://nvd.nist.gov/vuln/detail/CVE-2022-47112)

CVE-2022-29072 -7-Zip vulnerability

7-Zip through 21.07 on Windows allows privilege escalation and command execution when a file with the .7z extension is dragged to the Help>Contents area. This is caused by misconfiguration of 7z.dll and a heap overflow. The command runs in a child process under the 7zFM.exe process.

CVSS

CVSS v3.1 Base Score: 7.8 (High)
CVSS v3.1 Temporal Score: 6.7 (Medium)
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:R](#)

CVSS v4.0 Score: NVD assessment not yet provided.
CVSS v4.0 Vector: NVD assessment not yet provided.

CWE

CWE-787: Out-of-bounds Write

CVE

NVD Summary Link: [NVD - CVE-2022-29072](https://nvd.nist.gov/vuln/detail/CVE-2022-29072) (https://nvd.nist.gov/vuln/detail/CVE-2022-29072)

CVE-2024-26203 - Azure Data Studio Elevation of Privilege Vulnerability

CVSS

CVSS v3.1 Base Score: 7.3 (High)
CVSS v3.1 Temporal Score: 6.4 (Medium)
CVSS v3.1 Vector: [CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C](#)

CVSS v4.0 Score: NVD assessment not yet provided.
CVSS v4.0 Vector: NVD assessment not yet provided.

CWE

CWE-284: Improper Access Control

CVE

NVD Summary Link: [NVD - CVE-2024-26203](https://nvd.nist.gov/vuln/detail/CVE-2024-26203) (https://nvd.nist.gov/vuln/detail/CVE-2024-26203)

Mitigating factors

Refer to section “No, ABB had not received any information indicating that this vulnerability had been exploited in 800xA Systems, when this security advisory was originally issued.

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

7-Zip – An attacker needs to extract the file with the vulnerable version of 7-Zip or trick a user to click a link or download a malicious file and extract them.

Microsoft Azure Data Studio – An attacker needs to get into the system and open a malicious file or run code which could exploit this vulnerability.

In both scenarios, the attack will be less likely if the user has configured the system as per recommended guidelines.

Workarounds

Workarounds are specific measures that a user can take to help block an attack, for example, temporarily disabling the vulnerable feature may remove the exposure with well-known impact on functionality.

There are no workarounds. Uninstalling the affected third-party software fully eliminates the risk of vulnerabilities. Refer to the section 'Recommended immediate actions'.

Frequently asked questions

What is the scope of the vulnerability?

An attacker who successfully exploited 7-Zip vulnerabilities could plant malicious files outside the extraction directories potentially compromising the full system.

An attacker who successfully exploited Microsoft Azure Data Studio vulnerability could allow a local attacker with low-level privileges to escalate their access potentially gaining full control over the system by exploiting improper access control. The exploitability of this vulnerability is rated as less likely by Microsoft (<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26203>).

What causes the vulnerability?

The vulnerability is caused by presence of vulnerable versions of the third-party software (7-Zip and Microsoft Azure Data Studio).

Why is it recommended to remove third-party software instead of updating it to a newer version without known vulnerabilities?

The vulnerable third-party software is recommended for removal rather than updating because these applications are not required for the functioning of the mentioned products. Retaining unused software on a system is generally considered poor practice, as it can introduce unnecessary risks and maintenance overhead. Therefore, removal is advised to maintain a clean and secure environment. However, if a user chooses to keep such software installed, the responsibility for updating and maintaining it lies entirely with the user.

What is ABB 800xA History?

800xA History is the main Historian Component which seamlessly stores real time-data (process values, events) from the control system and processes the data as per user requirement and makes it available for further analysis.

What is ABB Batch Management?

Batch Management is powerful, flexible software used to configure, run, and manage Batch operations.

What is ABB Production Response History?

Production Response (PR) provides the functions for collecting, Storing, maintaining, viewing, and analyzing Batch Management Production Data.

What is ABB 800xA for Symphony Plus Harmony?

800xA for Symphony Plus Harmony provides connectivity to the Symphony Plus Distributed Control System (DCS). This connectivity is integrated with the 800xA Operator Workplace to provide a single operation and configuration view of the system.

What is ABB 800xA for AC 870P Melody?

The 800xA for AC 870P / Melody component connects the Control System AC 870P / Melody and 800xA Operations to a System 800xA distributed process management and control system.

What is ABB Application Change Management?

Application Change Management (ACM) is a version control tool used for engineering solutions in System 800xA. It is a configuration management system designed to handle configuration records. It also has the capability to be used as a configuration change reporting system.

What might an attacker use the vulnerability to do?

An attacker who successfully exploits 7-Zip vulnerabilities could plant malicious files outside the extraction directories potentially compromising the full system.

An attacker who successfully exploits Microsoft Azure Data Studio vulnerability allows a local attacker with low-level privileges to escalate their access, potentially gaining full control over the system by exploiting improper access control.

How could an attacker exploit the vulnerability?

An attacker could try to exploit vulnerability, by gaining control over the system and extracts a malicious file using this version of 7-Zip. Otherwise, the attacker must force the user to visit malicious websites or click links and extract the package through 7-zip.

Similarly Azure Data Studio improperly handles privileged commands. An attacker can abuse this gap to run malicious code with higher privileges.

Recommended practices help mitigate such attacks, see section Mitigating Factors above.

Could 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

What does the update do?

This is not an update. It is a recommendation to the customer to uninstall the vulnerable version of the software.

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

Yes, this vulnerability in the third-party software has 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 in 800xA Systems, when this security advisory was originally issued.

General security recommendations

Control systems and the control network are exposed to cyber threats. 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 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 Prevention 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 documents⁵:

- [3BDS011222D](#) System 800xA Reference - System Configuration
- [3BSE034463D](#) System 800xA Reference - Network Configuration
- [3BSE037410D](#) System 800xA Reference - Administration and Security
- [3BSE080520D](#) System 800xA Reference - Security Deployment Guide

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	31-03-2026

⁵ Access to listed documents might be restricted to customers having an active ABB Care Automation Software Maintenance agreement and a valid ABB MyControlSystem user ID.