DOCUMENT ID: 7PAA024620
REVISION:A
DATE:12/06/2026 2026-06-17

CYBER SECURITY ADVISORY

ABB Ability Edgenius: Copy Fail

CVE ID: CVE-2026-31431

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.

© Copyright 2026 ABB. All rights reserved.

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

ABB Ability Edgenius 3.2 all version of below products

- Edgenius Gateway - bE100
- Edgenius Gateway - E3100C
- Edgenius Server - vE1000

Vulnerability IDs and Product Issue Numbers (PIN)

CVE-2026-31431

Summary

ABB is aware of public reports of a vulnerability CVE-2026-31431 (Copy Fail) in the product versions listed above. An update is available that resolves a publicly reported vulnerability in the product versions listed above.

CVE-2026-31431 (Copy Fail) is a Linux kernel vulnerability that may allow a locally authenticated user or compromised container workload to gain elevated (root) privileges on affected systems. Once root access is obtained, the attacker can effectively gain complete control of the system

Recommended immediate actions

The problem is corrected in the following product versions:

© Copyright 2026 ABB. All rights reserved.

Edgenius 3.2.4.1

ABB recommends that customers apply the update at earliest convenience.

Vulnerability severity and details

The Linux kernel vulnerability CVE-2026-31431 (“Copy Fail”) affects Linux kernels used by most major Linux distributions released since 2017. As a result, Edgenius systems are also impacted.

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS)[1] for both v3.1[2] and v4.0[3].

The indicated Common Weakness Enumerations (CWE) have been selected from the MITRE CWE list[4].

CVE-2026-31431 “Copy Fail”

CVE-2026-31431 (Copy Fail) is a Linux kernel vulnerability that may allow a locally authenticated user or compromised container workload to gain elevated (root) privileges on affected systems. The issue originates in the Linux kernel’s cryptographic subsystem and impacts kernels used by most major Linux distributions released since 2017.

Successful exploitation requires local code execution, however, in shared, containerized, or multi-tenant environments this may increase the security risk

CVSS

CVSS v3.1 Base Score:	7.8 (High)
CVSS v3.1 Temporal Score:	Not assigned / Not available (NA)
CVSS v3.1 Vector:	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v4.0 Score	7.3 / High
CVSS v4.0 Vector:	CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

CWE

CWE-669: Incorrect Resource Transfer Between Spheres

CVE

NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2026-31431

[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/.

© Copyright 2026 ABB. All rights reserved.

Mitigating factors

Mitigating factors describe conditions and circumstances that make an attack that exploits the vulnerability difficult or less likely to succeed. Refer to section General security recommendations for further advise on how to keep your system secure. Recommended mitigation factors

- Limit access to ssh or cockpit
- By default, no additional lower privilege users are present on Edgenius installations

Frequently asked questions

What causes the vulnerability?

A flaw was found in the Linux kernel's algif_aead cryptographic algorithm interface. An incorrect 'in-place operation' was introduced, where the source and destination data mappings were different. This could lead to unexpected behavior or data integrity issues during cryptographic operations, potentially impacting the reliability of encrypted communications.

What is Edgenius?

ABB Ability™ Edgenius is an edge computing platform that

- Connects to control systems, devices, and equipment
- Collects and contextualizes operational data
- Hosts applications that deliver real-time insights and AI-driven recommendations

What might an attacker use the vulnerability to do?

Successful exploitation could enable a local user attacker to gain administrative control of the system node, execute arbitrary code, or cause the node to become unavailable.

How could an attacker exploit the vulnerability?

An attacker could exploit this vulnerability after obtaining local access to the system. By invoking the Linux kernel’s affected cryptographic interface (algif_aead), the attacker can trigger incorrect memory handling in the kernel. This allows the attacker to escalate privileges from a normal user to full administrative (root) access on the affected system node

Could the vulnerability be exploited remotely?

No, to exploit this vulnerability an attacker would need to have local access (physical access or through valid SSH credentials) to an affected system node.

What does the update do?

The update resolves the issue by incorporating the security update of the Linux kernel.

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

Yes, this vulnerability has been publicly disclosed.

© Copyright 2026 ABB. All rights reserved.

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 for Edgenius 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.

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		Initial version	06/12/2026

© Copyright 2026 ABB. All rights reserved.