DOCUMENT ID: 4JDE002044
REVISION: A
DATE: 2026-09-17

CYBER SECURITY ADVISORY

dynovaPRO™ Reset Credentials Vulnerability

CVE ID: CVE-2026-18963

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.

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

dynovaPRO™ cloud system before 2026-08-27 12:00 (CEST)

Vulnerability IDs

CVE-2026-18963

Summary

ABB is aware of public reports of a vulnerability in the product versions listed above. An update has been deployed to the cloud system that resolves a publicly reported vulnerability in the product versions listed above.

An attacker who successfully exploited this vulnerability could take remote control of the product.

The vulnerability has been identified in the keycloak authentication component which is integrated into dynovaPRO™. The vulnerability exists in the 'Forgot Password' functionality and allows unauthenticated attackers to bypass authentication and hijack user accounts.

Users who have received a password reset mail before the mentioned date, without having requested it, are thereby potentially attacked by exploiting this vulnerability.

ABB investigated potentially malicious user reset activities and blocked those user access immediately to reduce the exploitation risk. The credentials of those users have been deleted after the software fix was deployed and the users were informed that they must reset their password to gain access to dynovaPRO™ again.

Recommended immediate actions

The problem is corrected in the dynovaPRO™ cloud system since 2026-08-27 12:00 (CEST).

Users who have received a password reset mail without their consent should reset their password to ensure an attacker did not gain access to their account.

Vulnerability severity and details

A vulnerability exists in the component keycloak included in the product versions listed above. An attacker could exploit the vulnerability by sending a specially crafted message to the system, allowing the attacker to take control of the product.

An attacker requires only knowledge of the target user's email address to execute the attack. The attack process looks as follows:

- Attacker requests a password reset for a known user
- Password reset mail is being sent to the user
- Attacker can reset the password without having access to the password reset mail's link
- Attacker can login with the newly set password

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

The indicated Common Weakness Enumerations (CWE) have been selected from the MITRE CWE list[3].

CVE-2026-18963 keycloak-services: Unauthenticated account takeover via reset-credentials flow bypass

A flaw was found in the reset-credentials flow of the keycloak-services component, which is the core engine for identity and access management in Keycloak. The issue allows an unauthenticated attacker to force the password reset process for any user without needing to click the required email verification link. This can result in the attacker gaining full control over target user accounts by directly setting new credentials.

CVSS

CVSS v3.1 Base Score: 9.1 Critical
CVSS v3.1 Temporal Score: 8.4 High
CVSS v3.1 Vector:
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/E:F/RL:O/RC:C/CR:M/IR:M/AR:L/MAV:N/MAC:L/MPR:N/MUI:N/MS:U/MC:L/MI:L/MA:N

[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] Common Weakness Enumeration (CWE), The MITRE Corporation, https://cwe.mitre.org/.

CVSS v3.1 Environmental Score: 6.0 Medium

CWE
CWE-640: Weak Password Recovery Mechanism

CVE
NVD Summary Link: https://nvd.nist.gov/vuln/detail/cve-2026-18963

Mitigating factors

The following conditions reduce the risk of exploitation of this vulnerability:

- Limited Attack Surface: The vulnerability is specific to the password reset functionality. Other authentication methods are not affected.
- Email Notifications: Legitimate users receive email notifications during password reset attempts, which may alert them to unauthorized access attempts.

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

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. ABB has tested the following workarounds. Although these workarounds will not correct the underlying vulnerability, they can help block known attack vectors. When a workaround reduces functionality, this is identified below as “Impact of workaround”.

ABB has implemented temporary mitigation measures for customers:

- Password Reset Function disabled: The password reset functionality has been disabled for all dynovaPRO™ customers to prevent exploitation of this vulnerability as a short term step, until software update has been carried out.
- Account Monitoring: Users are advised to monitor their user account activity for any unauthorized access.

Note: These workarounds do not eliminate the underlying vulnerability until it has been fixed in dynovaPRO™.

Frequently asked questions

What causes the vulnerability?

The vulnerability is caused by improper token validation in the Keycloak password recovery mechanism, allowing attackers to bypass email verification and reset user credentials without proper authentication.

Which components are affected?

Keycloak authentication component integrated into dynovaPRO™ is affected.

What might an attacker use the vulnerability to do?

An attacker can take over user accounts by resetting credentials, gaining unauthorized access to personal and operational data, modifying system configurations, and potentially causing service disruptions, depending on the user's privileges.

How could an attacker exploit the vulnerability?

An attacker sends crafted HTTP requests to the password reset endpoint with manipulated session parameters, bypassing normal authentication and email verification. Only the user's email address is required.

Could the vulnerability be exploited remotely?

Yes, an attacker with network access to dynovaPRO™ can exploit this vulnerability remotely without any special conditions or physical access requirements.

Can functional safety be affected by an exploit of this vulnerability?

While functional safety systems are separate from user account management, compromise of administrative accounts could enable unauthorized control commands affecting operational devices such as chargers, batteries, and PV systems.

What does the update do?

The update corrects the Keycloak token validation mechanism in the password reset flow, ensuring proper authentication and email verification before allowing credential changes.

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

Yes, CVE-2026-18963 has been publicly disclosed at 17/08/2026 and is documented in the National Vulnerability Database (NVD).

When this security advisory was issued, had ABB received any reports that this vulnerability was being exploited?

As of August 27, 2026, ABB had not received confirmed reports of active exploitation in the wild. Internal log analysis identified 26 password change events affecting 9 customers, which may indicate testing or reconnaissance activity. Those users have been disabled and forced to reset their password after the software vulnerability fix has been deployed.

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 designed for such exposure and business requirements dictate it.
- 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.

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	all	Initial version	2026-09-17