DOCUMENT ID: 2CRT000009
REVISION: C
DATE: 2026-01-07

CYBER SECURITY ADVISORY

WebPro SNMP Card PowerValue Multiple Vulnerabilities

CVE IDs: CVE-2025-4675, CVE-2025-4676, CVE-2025-4677

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

Product	Version
• WebPro SNMP Card PowerValue • WebPro SNMP Card PowerValue UL	1.1.8.k and earlier

Vulnerability IDs

CVE IDs: CVE-2025-4675, CVE-2025-4676, CVE-2025-4677

Summary

ABB became aware of multiple internally discovered vulnerabilities in the **WebPro SNMP card PowerValue** product listed above.

Depending upon the vulnerability, an attacker with access to local network who successfully exploited this vulnerability could have

- Unauthorized access
- Insufficient Session Expiration leading to resource unavailability
- Uncontrolled Resource Consumption leading to DOS attack

ABB strongly advises customers to update the latest firmware of affected products.

Recommended immediate actions

The problem is corrected in the following product versions:

WebPro SNMP card PowerValue version 1.1.8.p

ABB advises users of the affected product versions to reach out to ABB Digital Service Support (ch.ups.digital@abb.com) for guidance and recommended actions.

Additionally, ABB recommends implementing defensive measures to reduce the risk of vulnerability exploitation, as outlined in the product instruction manual. Please refer to the section “Mitigation factors” for more information.

Vulnerability severity and details

ABB has become aware of multiple vulnerabilities.

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

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

No.	CVE ID	Title	
1	**CVE-2025-4675**	Improper implementation of Modbus protocol leading to DOS attack.	
	Description	Modus(slave) protocol was implemented incorrectly in the device, port 502 becomes unstable and Modbus service is unavailable until manual reboot of the device.	
	CWE	CWE-754: Improper Check for Unusual or Exceptional Conditions.	
	CVSS v3.1	Base Score:	6.5
		Temporal Score:	5.6
		Vector:	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:F/RL:O/RC:U
	CVSS v4.0	Score:	7.1

[1] 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.

[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.

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

		Vector:	CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N
	CVE NVD Summary Link	https://nvd.nist.gov/vuln/detail/CVE-2025-4675	
2	**CVE-2025-4676**	Authentication bypass by brute forcing Authentication Headers.	
	Description	Device web HMI authenticates user by validating the first character of the session cookie and authentication token. So, if only the first characters of the session cookie and token are correct, a user will be validated. An attacker can easily brute force the first character of both session cookie and bearer token. This vulnerability allows an attacker to easily bypass the authentication implemented on the device.	
	CWE	CWE-303: Incorrect Implementation of Authentication Algorithm.	
	CVSS v3.1	Base Score:	8.8
		Temporal Score:	7.5
		Vector:	CVSS:3.1/AV:A/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H/E:F/RL:O/RC:U
	CVSS v4.0	Score:	8.4
		Vector:	CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:H/SC:H/SI:H/SA:H
	CVE NVD Summary Link	https://nvd.nist.gov/vuln/detail/CVE-2025-4676	
3	**CVE-2025-4677**	Idle session timeout is not configured for multiple open ports.	
	Description	Idle session timeout is not configured for port 23 and 502 in device, due to which an attacker can make number of connections to the device and since device is not destroying the connections, it can lead to unavailability of the resources from the device.	
	CWE	CWE-613: Insufficient Session Expiration.	
	CVSS v3.1	Base Score:	6.5
		Temporal Score:	5.6
		Vector:	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:F/RL:O/RC:U
	CVSS v4.0	Score:	7.1
		Vector:	CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

	CVE NVD Summary Link	https://nvd.nist.gov/vuln/detail/CVE-2025-4677

Mitigating factors

Mitigating factors describe conditions and circumstances that make an attack that exploits the vulnerability difficult or less likely to succeed.

In case customer cannot opt for not to upgrade the firmware or it is not feasible then please immediately apply mitigating factors mentioned in “General security recommendations”.

Frequently asked questions

What causes the vulnerability?

The vulnerabilities are caused by code defects allowing the attacker to do various unintended, unauthorized actions on the target device. Please look at the description of the respective vulnerabilities in section “*Vulnerability severity and details*” for further details.

What is WebPro SNMP Card PowerValue?

The **WebPro SNMP Card PowerValue** provide web server to monitor and manage multiple UPS products in networked environment. It can detect temperature and humidity for the environment via connecting to EMD (Environmental Monitoring Device). It can not only prevent data loss from power outage and safely shutdown systems but also store programming data and scheduled shut down the UPS. All UPS warning and fault event records can be kept in **WebPro SNMP Card PowerValue**.

What might an attacker use the vulnerability to do?

If mentioned vulnerabilities have been successfully exploited by an attacker, this could allow the attacker to take control of the target **WebPro SNMP Card PowerValue** device.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by creating a specially crafted message and sending the message to **WebPro SNMP Card PowerValue** device. This 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 security system.

Could the vulnerability be exploited remotely?

Yes, an attacker who has network access to an affected system node could exploit this vulnerability. Recommended practices include that User’s network systems are physically protected, have no direct connections to the Internet nor any other untrusted network, and are separated from other networks by means of a firewall system that has a minimal number of ports exposed.

What does the update do?

WebPro SNMP Card PowerValue v1.1.8.p update has fixes for all the vulnerabilities mentioned in “ ***Vulnerability severity and details***” section.

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

No, the vulnerabilities have not 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 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 programming 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 Digital Service Support ch.ups.digital@abb.com. For contact information, see www.abb.com/contactcenters.

Information about ABB’s cyber security program and capabilities can be found at https://go.abb/cybersecurity.

Revision history

Rev. Ind.	Page (p) Chapter (c)	Change description	Rev. date
C	all	Initial version	07-Jan-2026