DOCUMENT ID: 2CMT006108
REVISION: A
DATE: 2024-06-03

CYBER SECURITY ADVISORY

ABB WebPro SNMP card PowerValue Cross-Site Scripting (XSS) vulnerability

ABBVREP0138

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

Affected product	Versions
• WebPro SNMP card PowerValue • WebPro SNMP card PowerValue UL	1.1.8.j and earlier

Vulnerability IDs

ABBVREP0138

Summary

A software update is available that resolves a privately reported vulnerability in the SNMP Card versions listed above. The version number of the update is SNMP Web Pro v1.1.8.k.

An attacker with admin privileges who successfully exploits this vulnerability by injecting and executing malicious script on the user browsers, could take control of the SNMP Card and insert and run arbitrary code. Attacker that successfully exploits this vulnerability of the SNMP card can potentially send a shutdown command to the UPS, causing denial of service of the UPS.

Recommended immediate actions

The problem is corrected in the following product version:

SNMP Web Pro v1.1.8.k

ABB recommends that customers apply the update at earliest convenience. For more information, please get in contact with Digital Service Support ch.ups.digital@abb.com.

Vulnerability severity and details

A vulnerability exists in the SNMP Card included in the product versions listed above. An attacker with admin privileges that successfully exploits this vulnerability by injecting and executing malicious script on the user browsers, allowing the attacker to take control of the product and insert and run arbitrary code. Attacker that successfully exploits this vulnerability of the SNMP card can potentially send a shutdown command to the UPS, causing denial of service of the UPS.

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

ABBVREP0138 Cross-Site Scripting (XSS) vulnerability

CVSS v3.1 Base Score:	9.1 (Critical)
CVSS v3.1 Temporal Score:	8.2 (High)
CVSS v3.1 Vector:	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C

Mitigating factors

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 exploits this vulnerability may draw users into taking actions, leading to sensitive data being leaked and potentially used as part of other attacks, thereby endangering the device.

What causes the vulnerability?

The name parameter used to send data using the get request method in the application has not been checked for compliance. The payload included as the parameter is immediately returned by the web application.

What is affected product?

- WebPro SNMP card PowerValue
- WebPro SNMP card PowerValue UL

What might an attacker use the vulnerability to do?

An attacker who successfully exploits this vulnerability may draw users into taking actions, leading to sensitive data being leaked and potentially used as part of other attacks, thereby endangering the device.

How could an attacker exploit the vulnerability?

Attackers can directly use URLs for requests, which may introduce malicious scripts in the name parameter of the request. The application responds and executes the script. Attacker that successfully exploits this vulnerability of the SNMP card can potentially send a shutdown command to the UPS, causing denial of service of the UPS.

Could the vulnerability be exploited remotely?

Yes, an attacker who has network access to an affected system node could exploit this vulnerability.

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

If the attacker successfully obtains sensitive information entered by the user, such as application passwords. This will result in the device being exposed and subjected to arbitrary operation.

What does the update do?

Purify the input parameter request, which must be on the whitelist. If not, filter it out directly. Another protective measure is that the request must carry a valid token, otherwise it will be ignored.

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

No, ABB received information about this vulnerability through responsible disclosure.

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 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.
- It is highly recommended to use secure protocols only. For example, use HTTPS protocol with authentication. HTTPS runs over the TLS protocol using public keys to enable shared data encryption.
- 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	all	Initial version	2024-06-03