ABB DOC ID: 9ADB005557_ABB_02
REVISION: 4
DATE: 2019-12-05

CYBER SECURITY ADVISORY

Weak Session Management in Data Logger Web Server

ABBVU-EPSO-201802

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.

Affected Products

ABB PVI-AEC-EVO Data Logger

Versions 0.2.19, 0.2.20, 0.2.22, 0.2.23, 0.3.20

Vulnerability ID

ABB ID: ABBVU-EPSO-201802

Summary

ABB is aware of public reports of a vulnerability in the product versions listed above. An attacker who successfully exploited this vulnerability could have access to local Web Interface and change parameters

At the moment, there are no plans of corrective measures for this specific issue in the affected product

Vulnerability Severity

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

Weak Session Management:

CVSS v3 Base Score:	5.5
CVSS v3 Temporal Score:	5.4
CVSS v3 Vector:	AV:A/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L/E:F/RL:U/RC:C
CVSS v3 Link:	https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:A/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L/E:F/RL:U/RC:C&version=3.1 https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L/E:F/RL:U/RC:C

Recommended immediate actions

Customers using PVI-AEC-EVO Data Logger are aware of the product discontinuity and advised to use latest ABB Data loggers.

Vulnerability Details

A vulnerability exists in the WebServer included in the product ABB PVI-AEC-EVO Data Logger and its versions listed above.

An attacker can gain access to the WebServer by sending a specially craft message during the period a valid user is accessing the device.

An attacker who successfully exploited this vulnerability could allow the attacker to read information of the solar plant and to change ABB PVI-AEC-EVO Data Logger parameters.

Mitigating Factors

Recommendation is to use the product in a local network and to not give public access to it from internet by, for example, exposing it with a NAT or equivalent solution. This reduce the risk as access to local network would be required to exploit this vulnerability.

Recommended security practices and firewall configurations can help protect a process control network from attacks that originate from outside the network. Such practices include that process control systems are physically protected from direct access by unauthorized personnel, 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, and others that must be evaluated case by case. Process control systems should not be used for Internet surfing, instant messaging, or receiving e-mails. Portable computers and removable storage media should be carefully scanned for viruses before they are connected to a control system.

Workarounds

No workaround is currently available for the user.

Frequently Asked Questions

What is the scope of the vulnerability?

An attacker who successfully exploited this vulnerability could gain access to the Webserver of the device.

What causes the vulnerability?

The vulnerability is caused due to non-usage of random Session ID for the Webserver of the ABB PVI-AEC-EVO Data Logger.

What is Weak Session Management in Data Logger?

The Webserver is the access to the data visualization and configuration of the ABB PVI-AEC-EVO Data Logger.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could allow the attacker to read information of the solar plant and to change ABB PVI-AEC-EVO Data Logger parameters including network ones; in this case the attacked could put the ABB PVI-AEC-EVO Data Logger out of the local network. The user can recover the situation by accessing the device (knowing its local IP) or by the local display.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by creating and sending a special message and sending the message to an affected system node. 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 firewall, or that he installs malicious software on a system node or otherwise infects the network with malicious software. Recommended practices help mitigate such attacks, see section Mitigating Factors above.

Could the vulnerability be exploited remotely?

No, an attacker without access to the local network that hosts the device cannot exploit the attack.

However, if the local network is exposed to the attacker through i.e. VPN, NAT, tunnel, IPSec or equivalent, the attack could be exploited. This is not due to the device itself but to the bad protection of the network itself.

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. Anyway, mapping the device on direct internet access is not a recommended practice.

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

Acknowledgements

ABB thanks the following for working with us to help protect customers:

Maxim Rupp for discovering this vulnerability.

Support

For additional information and support please contact your local ABB service organization. For contact information, see https://new.abb.com/contact-centers.

Information about ABB's cyber security program and capabilities can be found at www.abb.com/cybersecurity.