Security Advisory

Access Easy Controller 2.1 – 28. February 2019

CWE-287: Improper Authentication

(CVSS v3 Base Score: 6.5)

1 Overview and Management Summary

Independent researcher Maxim Rupp identified a vulnerability in the web-based interfaces of Access Easy Controller (AEC).

Access Easy Controller uses the gSOAP service to retrieve the real-time event, and the sensor status for the client browsers. If a malicious user gets to know the SOAP endpoint URL, they will be able to access the AEC resources using the SOAP API interface without user authorization.

2 Technical Details

2.1 Affected Products

Access Easy Controller 2.1

2.2 CVSS Rating

The CVSS V3 Base Score is rated at: 6.5 (Medium) CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L

Vulnerability classification has been performed using the CVSSv3 scoring system http://www.first.org/cvss/.

The CVSS environmental score is specific to each customer’s environment and should be defined by the customer to attain a final scoring.

3 Solution

To fix this issue in Access Easy Controller, a token-based handshake mechanism is introduced between the client and AEC server. If the user wants to get AEC real-time events and I/O status, the user must login with a valid credential to the web client. Without it, SOAP services access will be denied for this request. After successful login into the web client, if the user wants to access the AEC real-time events and I/O status via SOAP API using third-party application, the user has to send the SOAP request with the AEC server generated token, session code and the SOAP request must come from the same IP address from the current web client logged in. If there is a mismatch, the AEC server will send the SOAP error for the SOAP service request. The AEC server token will be refreshed and a new token will be generated in a predefined interval based on the web client request. If any web client request comes with the expired token, then the server will reject the SOAP service request. Once the current logged-in user has logged out from the AEC server, the SOAP service resource access will be denied. Firmware AEC 2.1.9.3 that fixes this vulnerability was released on 1 Nov 2018.

4 Acknowledgments

Bosch thanks Maxim Rupp for identifying the vulnerability and working with Bosch.

5 Additional Resources

1. Patch download
2. For further inquiries on vulnerabilities in Bosch products and solutions, please contact the Bosch PSIRT: https://psirt.bosch.com

6 Document Changelog

2018.12.03 – Revision 1.00: Initial Publication

2019.01.08 – Revision 1.01: Updated CVSS Score

2019.02.28 – Revision 1.02: Patch download link corrected

pki, BOSCH, DE, B, T, BT.ProVIRT

Digitally signed by pki, BOSCH, DE, B, T, BT.ProVIRT Date: 2019.02.28 17:51:52 +01'00'