Security Advisory: Unauthorized access to sensitive data

Software vulnerability for Access Professional Edition 3.7 downwards – September 11th, 2019

BOSCH-SA-710832-BT

CVE-2019-11898 (CVSS Score: 9.9)

1 Overview and management summary

A discovered security vulnerability affects Access Professional Edition (APE) installations of versions 3.7 downwards.

The vulnerability enables unauthorized access to sensitive data of the APE system.

In cases where a software update is not possible, a reduction in the system's network exposure is advised. Internet-accessible installations should be firewalled, whilst additional steps like network isolation by VLAN, IP filtering features of the devices and other technologies should be used to decrease the exposure of vulnerable systems. In addition, the SMB service should be properly configured to Microsoft's latest security recommendations.

The vulnerability was discovered and disclosed to Bosch in a coordinated manner by the external researcher, Oleksii Orekhov.

2 Technical details

2.1 Vulnerability classification and solution approach

CVE-2019-11898: Unauthorized APE administration privileges can be achieved by reverse engineering one of the APE service tools. The service tool is discontinued with APE 3.8.

2.2 CVSS rating

- CVE-2019-11898
  The CVSS v3 Base Scores for the support tool vulnerability are rated at: 9.9 (Critical)
  CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

2.3 Impact

The vulnerability can be used to achieve unauthorized access to sensitive data of the APE system. This could enable a potential attacker to get unauthorized access to the site. Necessary prerequisite for this attack is access to the network of the APE server.

3 Vulnerability fix

3.1 Software updates

The recommended approach is to update the software to a fixed version as soon as possible. Until a fixed software version is installed, the mitigation approaches firewalling, and IP filtering can be utilized.

A fixed APE version is available on the Bosch Product Catalog.

3.2 Network configuration

We advise a reduction of network exposure of the system. Systems that are accessible via the internet should be firewalled. The SMB service in Microsoft Windows should be properly configured to Microsoft's latest security recommendations.
Additional measures such as network isolation via VLAN, or the filtering of systems IP features and supplementary technology, are strongly advised.

4 Direct links

The referenced software (see Appendix A) is provided on the Bosch Product Catalog.

- Software updates: Bosch Product Catalog - APE
- Bosch Building Technologies Security Advisory page
- Secure Operation Concept
- Bosch PSIRT

5 Document changelog

2019 – 09 – 11 – Revision 1.00: Initial release

Appendix A: List of affected products and fixed Software Versions

Access Professional Edition (APE)	
Software	Fixed software version
Earlier Versions of APE (APE 3.7 and downwards)	upgrade to APE 3.8 or higher

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

Digitally signed by pki, BOSCH, DE, B, T, BT.ProVIRT
Date: 2019.09.11 11:36:34 +02'00'