Security Advisory

DIVAR 400 & 600 series Vulnerability – January 2019

CVSS v3 Base Score: 10

1 Overview and Management Summary

Two issues have been discovered affecting the Bosch digital recorder DIVAR 400 & 600 series, which do not reflect current state-of-the art technology. These issues apply to recorders which are connected to an open network.

Bosch strongly recommends to operate the digital recorder DIVAR 400 & 600 series in a closed network. The mentioned vulnerabilities do not apply as long as the recorder is operated in a closed network.

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

2 Technical Details

2.1 Vulnerability Classification and Solution Approach

These vulnerabilities are classified as ‘Improper Access Control’ and ‘Unprotected Credentials’. It is accordingly ranked as “CWE-284: Improper Access Control” and “CWE-522: Insufficiently Protected Credentials”.

2.2 CVSS Rating

Improper Access Control: 5.3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Unprotected Credentials: 10

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Vulnerability classification is performed using the CVSSv3 scoring system. The CVSS environmental score is specific to each customer’s environment and should be determined by the customer to attain a final scoring.

2.3 Impact

The affected products are Bosch digital recorder DVR 400 & 600 series. These products were announced end of life in 2014.

The first issue, improper access control, concerns the ability to access information in the application without authenticating. By accessing a specific uniform resource locator (URL) on the built-in webserver, a malicious user might able the access information in the application.

The second issue is that passwords are presented in a file that is accessible without authentication. In addition to that, the administrator credentials could be acquired by XML injection of the shell code. It is important to note that this issue is severe; when obtaining the administrator credentials, root access can be acquired and the availability system is at risk.

3 Workaround

3.1 Closed network

Bosch strongly recommends to operate the digital recorder DVR 400 & 600 series in a closed network. The above vulnerabilities do not apply as long as the recorder is operated in a closed network.

3.2 Upgrade hardware

Customers who want to operate their recorder in an open network are strongly advised to update their recorder to the latest Bosch recording portfolio (DIVAR Hybrid and Network recording solutions).

4 Direct Link

Security Advisory: https://media.boschsecurity.com/fs/media/pb/security_advisories/bosch-2019-0101-bt_security_advisory_divar_400_600.pdf

5 Document Changelog

2018.10.22 – Revision 0.1: Initial Draft

2019.01.09 – Revision 1.0: Final version

2019.01.18 – Revision 1.1: Corrected CVSS rating for 'Improper Access Control: 5.3'

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

Digitally signed by pki, BOSCH, DE, B, T, BT.ProVIRT
Date: 2019.01.22 11:51:29 +01'00'