Security Advisory: Unauthenticated Certificate Access

Video Recording Manager Vulnerability – 2019 May 9th

BOSCH-SA-804652-BT

CVE-2019-11684 (CVSS v3 Base Score: 9.9)

1 Overview and Management Summary

A recently discovered security vulnerability affects the Bosch Video Recording Manager (VRM) software. The VRM software is commonly installed as a component in Bosch Video Management Systems (BVMS) and included in DIVAR IP 5000 devices. The vulnerability potentially allows unauthenticated access to a limited subset of certificates. The affected certificates are stored in the operating systems certificate store. The vulnerability is exploitable via the network interface. Bosch rates this vulnerability at 9.9 (Critical) and recommends customers to update vulnerable components with fixed software versions.

- As of 2019 May 9th, updated firmware files are published on the Bosch Download Store (Link).
- As of 2019 May 9th, there is currently no indication that the vulnerability is either publicly known or utilized.

If a software update is not possible in a timely manner, a reduction in the systems network exposure is advised. Internet-accessible systems should be firewalled. Additional protective steps like network isolation by VLAN, IP filtering features of the devices and other technologies can be used to further decrease the exposure of vulnerable devices.

The vulnerability was discovered during internal product tests.

2 Technical Details

2.1 Vulnerability Classification and Solution Approach

This vulnerability is classified as “CWE-284: Improper Access Control.” The affected RCP+ server of the VRM component allows arbitrary and unauthenticated access to a limited subset of certificates, stored in the underlying Microsoft Windows operating system. The fixed versions implement modified authentication checks. The vulnerability resides in the software from VRM version 3.70. Prior releases of VRM software are considered unaffected.

2.2 CVSS Rating

The CVSS v3 Base Score is rated at: 9.9 (Critical) CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:H/A:L

2.3 Impact

The vulnerability can be utilized to add, modify or delete a subset of certificates, located in the certificate store of the underlying Microsoft Windows operating system. The impact is considered limited to certificates of the “Local System” access level. Based on the possibility, that additional customer installed software on the target system relies on the shared certificate store of “Local System”, the CVSS scope is rated with “Changed”. Attacks on out of scope certificates, e.g. operating system certificate stored with “Machine Level” rights, can result in a temporary freeze of VRM components.

The Attack Vector is executable via ports 80 (http) and 443 (https) at the network level. A non-exhaustive list of application relevant assets includes certificates for recording encryption and VRM SSL webserver certificates. The modification of certificates for recording encryption can result in recorded video data, which are not accessible to the designated operator. Thus video data recorded after the recording encryption certificate manipulation could be lost. The successful modification of the VRM webserver SSL certificate can fulfill a baseline requirement for subsequent Man-In-The-Middle (MITM) attacks.

3 Vulnerability Fix

3.1 Software Updates

The recommended approach is to update the software of affected Bosch products to a fixed version. If an update is not possible in a timely manner, the mitigation approaches Firewalling and IP Filtering can be utilized. A list of affected and fixed software versions is available in the “Affected Hardware” and “Affected Software” chapter of this document.

4 Mitigations and Workarounds

4.1 Firewalling (Network)

It is advised that the devices should not be exposed directly to the internet or other insecure networks. This includes port-forwarding, which would not protect devices adequately. Firewalling a device significantly reduces its attack surface.

4.2 IP Filtering (Device)

As an additional supporting measure in shared environments, internal IP filters of BVMS Systems can be activated. This allows the device to whitelist IPs and IP-ranges. IPs not included in these ranges cannot connect, and therefore not exploit this vulnerability.

5 Affected Hardware

5.1 Bosch DIVAR IP 5000

For Bosch DIVAR IP 5000 the following fixed firmware versions are suggested:

DIVAR IP 5000 versions	Vulnerable versions (until and including)	Fixed or non-vulnerable firmware versions (and later)
3.62	N/A	3.62 and prior
3.80	3.80.0033, 3.80.0035, 3.80.0037	3.80.0039

6 Affected Software

6.1 Video Recording Manager (VRM)

For Bosch Video Recording Manager (VRM) the following fixed VRM versions are suggested:

VRM versions	Vulnerable versions (until and including)	Fixed or non-vulnerable VRM versions (and later)
<=3.62	N/A	3.10, 3.20, 3.21, 3.50, 3.51, 3.55, 3.60, 3.61, 3.62
3.70	3.70.0056, 3.70.0058, 3.70.0060, 3.70.0062	N/A (update to 3.71.0034)
3.71	3.71.0022, 3.71.0029, 3.71.0031, 3.71.0032	3.71.0034
3.81	3.81.0032, 3.81.0038, 3.81.0048	3.81.0050

6.2 Bosch Video Management System (BVMS)

For Bosch Video Management Systems (BVMS) the following fixed VRM versions are suggested:

BVMS versions	Vulnerable versions (until and including)	Fixed or non-vulnerable VRM versions (and later)
6.0	N/A	3.50
7.0	N/A	3.55
7.5 [sic]	N/A	3.60
7.5 [sic]	3.70.0056, 3.70.0058, 3.70.0060, 3.70.0062 3.71.0022, 3.71.0029, 3.71.0031, 3.71.0032	3.71.0034
8.0		
9.0	3.81.0032, 3.81.0038, 3.81.0048	3.81.0050

7 Direct Links

Software Updates:
https://downloadstore.boschsecurity.com

Release Letters:
https://downloadstore.boschsecurity.com/FILES/Bosch_Releaseletter_VRM_3.71.0034.pdf
https://downloadstore.boschsecurity.com/FILES/Bosch_Releaseletter_VRM_3.81.0050.pdf
https://downloadstore.boschsecurity.com/FILES/Bosch_Releaseletter_DIP5000_3_80_0039.pdf

Note:
For specific software versions, which are not available in the Bosch Download Area, please contact your Bosch Support.

8 Document Change Log

2019.05.09 – Revision 1.00: Initial Release
2019.05.22 – Revision 1.01: Updated link to the Bosch Release letter VRM 3.71.0034

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

Digitally signed by pki, BOSCH, DE, B, T, BT.ProVIRT
Date: 2019.05.22 11:33:21 +02'00'