Security Advisory: Path Traversal

Video Recording Manager vulnerability – April 2019

BOSCH-2019-0402-BT

CVE-2019-8952 (CVSS v3 Base Score: 4.9)

1 Overview and management summary

A recently discovered security vulnerability affects several Bosch software applications and hardware systems. It potentially allows, after authorization, the access to arbitrary files on the system via the network interface. Bosch rates this vulnerability at CVSS v3.0 4.9 (Medium) and recommends customers to upgrade devices with fixed software versions.

- As of 2019-04-03, updated firmware files are published on the Bosch Download Area (Link).
- As of 2019-04-03, there is currently no indication that the exploitation code 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, 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 devices.

The vulnerability was discovered and responsibly disclosed to Bosch by the external researcher Adrián Quirós Godoy.

2 Technical details

2.1 Vulnerability classification and solution approach

This vulnerability is classified as ‘Path Traversal’ and is located in the webserver. It is accordingly ranked as “CWE-28: Path Traversal: '..\filedir'”. The server fix utilizes additional input neutralization checks. The vulnerability resides in the software since version 3.10. The vulnerability is fixed in version 3.80 or higher. Prior versions are considered unaffected.

2.2 CVSS rating

The CVSS v3 Base Score is rated at: 4.9 (Medium) CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N

2.3 Impact

The vulnerability can be used to remotely traverse through the file system to access files or directories that are outside of the restricted directory. This would enable a potential attacker, for example, to access restricted files on the target system. A necessary prerequisite for this attack is the network access to the webserver (HTTP / HTTPS) of the device and valid user credentials. An affected system should be secured by updating to a fixed version and changing passwords.

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 approach Firewalling can be utilized. A list of affected devices 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.

5 Affected hardware

5.1 Bosch DIVAR IP 2000

For the Bosch DIVAR IP 2000 the following fixed firmware versions are suggested:

- Vulnerable versions: 3.10, 3.20; 3.21; 3.50; 3.51; 3.55; 3.60; 3.61; 3.62
- Fixed versions: 3.62.0019 (and newer)

5.2 Bosch DIVAR IP 5000

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

- Vulnerable version: 3.10 3.20; 3.21; 3.50; 3.51; 3.55; 3.60; 3.61; 3.62
- Fixed version: 3.80.0033 (and newer)

6 Affected software

6.1 Video Recording Manager (VRM)

For the VRM the following fixed software versions are suggested:

- Vulnerable version: 3.10, 3.20; 3.21; 3.50; 3.51; 3.55; 3.60; 3.61; 3.62; 3.70; 3.71 (except 3.71.0032 and newer)
- Fixed version: 3.71.0032; 3.81.0032 (and newer)

6.2 Bosch Video Management System (BVMS)

For the BVMS the following fixed firmware versions are suggested:

BVMS Version	Vulnerable VRM Version (until and including)	Fixed VRM Version (and later)
6.0	3.50.00XX	Upgrade to BVMS 7.5
6.5	3.55.00XX	Upgrade to BVMS 7.5
7.0	3.60.00XX	Upgrade to BVMS 7.5
7.5	3.60.00XX	3.71.0032
7.5	3.70.0056	3.71.0032
8.0	3.70.0056	3.71.0032
9.0	3.81.0032 (Not vulnerable)	

7 Related advisories

CVE-2019-8951 (CVSS v3 Base Score: 6.1): Minimum VRM Version 3.81.0032

8 Direct links

- Software updates: Bosch Download Area
- Bosch Building Technologies Security Advisory page
- Hardening Guide
- Bosch PSIRT Security Advisory

9 Document changelog

2019 – 04 – 03 – Revision 1.00: Initial release

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

Digitally signed by pki, BOSCH, DE, B, T, BT.ProVIRT
Date: 2019.04.03 10:00:24 +02'00'