Security Advisory

IP Camera Vulnerability – 12. December 2018

CVE-2018-19036 (CVSS v3 Base Score: 9.4)

1 Overview and Management Summary

A recently discovered security vulnerability affects several Bosch IP cameras. It potentially allows the unauthorized execution of code on the device via the network interface. Bosch rates this vulnerability at 9.4 (Critical) and recommends customers to upgrade devices with updated firmware versions.

As of 2018-12-11, updated firmware files are published on the Bosch Download Store (Link).
As of 2018-12-12, there is currently no indication that the exploitation code is either publicly known or utilized.

If a firmware update is not possible in a timely manner, a reduction in the devices' network exposure is advised. Internet-accessible Bosch IP cameras 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 disclosed to Bosch in a coordinated manner by the external researcher, VDOO.

2 Technical Details

2.1 Vulnerability Classification and Solution Approach

This vulnerability is classified as 'buffer overflow', located in the RCP+ parser of the webserver. It is accordingly ranked as "CWE-120: Buffer Copy without Checking Size of Input". The parser fix utilizes additional input and target-buffers checks. The vulnerability resides in the firmware since version 6.32. Prior firmware versions are considered unaffected.

2.2 CVSS Rating

The CVSS V3 Base Score is rated at: 9.4 (Critical) CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H

2.3 Impact

The vulnerability can be used to remotely execute code on the device (RCE). This would enable a potential attacker, for example, to bypass access restrictions (e.g. username / password) or to reactivate disabled features (e.g. telnet). A necessary prerequisite for this attack is the network access to the webserver (HTTP / HTTPS) of the device. Despite its critical rating, possible attacks are considered incapable of accessing private keys if they are stored on the devices' Trusted Platform Module (TPM). An affected camera can be restored to its original state by the factory reset button.

3 Vulnerability Fix

3.1 Firmware Updates (Device)

The recommended approach is to update the firmware of affected Bosch IP cameras to a fixed version. If an update is not possible in a timely manner, the mitigation approaches Certificate Based Authentication, Firewalling, and IP Filtering can be utilized. A list of affected devices and fixed firmware versions is available in appendix A of this document.

4 Mitigations and Workarounds

4.1 Certificate Based Authentication (Device)

Starting with Release 6.40.0240, the "unauthenticated" aspect of the vulnerability can be mitigated to "authenticated" by enabling certificate-based authentication and executing additional hardening steps. After an initial certificate authentication

setup, additional hardening is mandatory for secure operation: Disable port 80, disable HSTS-redirect, and disable password authentication. This enforces the webserver to demand a valid client-certificate during the initial TLS-Handshake.

4.2 Firewalling (Network)

It is also 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.

4.3 IP Filtering (Device)

As further supporting measure in shared environments, the devices' internal IP filter can be activated. It allows the device to whitelist IPs and IP-ranges. IPs not included in these ranges cannot connect, and therefore not exploit this vulnerability.

5 BVMS

For the Bosch Video Management System (BVMS) the following fixed firmware versions are suggested:

CVE-2018-19036				
BVMS	**CPP7.3**	**CPP7**	**CPP6**	**CPP4**
7.0	6.44.0027	6.44.0027	6.44.0027	6.44.0027
7.5				
8.0				
9.0	6.51.0028	6.51.0028	6.51.0028	6.51.0028

6 Direct Links

Firmware Updates:
https://downloadstore.boschsecurity.com/index.php?type=FW

Hardening Guides:
https://resource.boschsecurity.com/documents/Data_Security_Guideb_Special_enUS_9007221590612491.pdf

Security Advisory:
https://media.boschsecurity.com/fs/media/pb/security_advisories/bosch-2018-1202-bt-cve-2018-19036_security_advisory_ip_camera_vulnerability.pdf

BVMS compatibility overview:
https://community.boschsecurity.com/varuj77995/attachments/varuj77995/bt_community-tkb-video/16/2/BVMS%209.0%20-%20Device%20compatibility.pdf

7 Document Changelog

2018.12.12 – Revision 1.02: Initial Release
2018.12.12 – Revision 1.03: Updated FW Versions

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

Digitally signed by pki, BOSCH, DE, B, T, BT.ProVIRT
Date: 2018.12.12 11:21:27 +01'00'

Appendix A: List of Affected Hardware and fixed Firmware

Common Product Platform 7.3 (CPP7.3)	
Product family	Firmware Version
AUTODOME IP 4000i	6.51.0028 6.50.0133 6.44.0027
AUTODOME IP 5000i	
AUTODOME IP starlight 5000i (IR)	
AUTODOME IP starlight 7000i	
DINION IP bullet 4000i	
DINION IP bullet 5000i	
DINION IP bullet 6000i	
FLEXIDOME IP 4000i	
FLEXIDOME IP 5000i	
MIC IP starlight 7000i	
MIC IP fusion 9000i	

Common Product Platform 7 (CPP7)	
Product family	Firmware Version
DINION IP starlight 6000	6.51.0028 6.50.0133 6.44.0027
DINION IP starlight 7000	
FLEXIDOME IP starlight 6000	
FLEXIDOME IP starlight 7000	
DINION IP thermal 8000	

Common Product Platform 6 (CPP6)	
Product family	Firmware Version
DINION IP starlight 8000 12MP	6.51.0028 6.50.0133 6.44.0027
DINION IP ultra 8000 12MP	
DINION IP ultra 8000 12MP with C/CS mount telephoto lens	
FLEXIDOME IP panoramic 7000 12MP 180	
FLEXIDOME IP panoramic 7000 12MP 360	
FLEXIDOME IP panoramic 7000 12MP 180 IVA	
FLEXIDOME IP panoramic 7000 12MP 360 IVA	
AVIOTEC IP starlight 8000	
FLEXIDOME IP panoramic 6000 12MP 180	
FLEXIDOME IP panoramic 6000 12MP 360	
FLEXIDOME IP panoramic 6000 12MP 180 IVA	
FLEXIDOME IP panoramic 6000 12MP 360 IVA	

Common Product Platform 4 (CPP4)	
Product family	Firmware Version
AUTODOME IP 4000 HD	6.51.0028 6.50.0133 6.44.0027
AUTODOME IP 5000 HD	
AUTODOME IP 5000 IR	
AUTODOME IP 7000 series	
DINION HD 1080p	
DINION HD 1080p HDR	
DINION HD 720p	
DINION imager 9000 HD	
DINION IP bullet 4000	
DINION IP bullet 5000	
DINION IP 4000 HD	
DINION IP 5000 HD	
DINION IP 5000 MP	
DINION IP starlight 7000 HD	
EXTEGRA IP dynamic 9000	
EXTEGRA IP starlight 9000	
FLEXIDOME corner 9000 MP	
FLEXIDOME HD 1080p	
FLEXIDOME HD 1080p HDR	
FLEXIDOME HD 720p	
Vandal-proof FLEXIDOME HD 1080p	
Vandal-proof FLEXIDOME HD 1080p HDR	
Vandal-proof FLEXIDOME HD 720p	
FLEXIDOME IP panoramic 5000	
FLEXIDOME IP indoor 5000 HD	
FLEXIDOME IP indoor 5000 MP	
FLEXIDOME IP indoor 4000 HD	
FLEXIDOME IP indoor 4000 IR	
FLEXIDOME IP outdoor 4000 HD	
FLEXIDOME IP outdoor 4000 IR	

Common Product Platform 4 (CPP4)	
Product family	Firmware Version
FLEXIDOME IP micro 5000 HD	6.51.0028 6.50.0133 6.44.0027
FLEXIDOME IP micro 5000 MP	
FLEXIDOME IP outdoor 5000 HD	
FLEXIDOME IP outdoor 5000 MP	
FLEXIDOME IP micro 2000 HD	
FLEXIDOME IP micro 2000 IP	
IP bullet 4000 HD	
IP bullet 5000 HD	
IP micro 2000	
IP micro 2000 HD	
MIC IP dynamic 7000	
MIC IP starlight 7000	
TINYON IP 2000 family	