Security Advisory: Side Channel Key Extraction

IP Cameras & Encoders Vulnerability – March 2021

BOSCH-SA-762869-BT

CVE-2021-3011 (CVSS v3.1 Base Score: 4.2)

1 Overview and Management Summary

A recently discovered side channel attack for the NXP P5x security microcontrollers was made public. It allows attackers to extract an ECDSA private key after extensive physical access to the chip. The P5x is used as secure certificate storage on Bosch cameras and encoders built on platforms CPP-ENC, CPP3, CPP4, CPP5, CPP6, CPP7 and CPP7.3.

Bosch does not include any ECDSA keys from factory, but ECDSA keys can be installed or generated by the customer. Only the private key of the affected camera can be obtained by the attacker.

Bosch rates this vulnerability with a CVSS v3.1 Base Score of 4.2 and recommends customers to take a risk-based approach at using ECDSA keys and considering listed mitigations.

The vulnerability was discovered by security researchers Victor Lomne and Thomas Roche and disclosed by NXP to Bosch.

2 Technical Details

2.1 Vulnerability Classification and Solution Approach

This vulnerability is classified as “CWE-203: Observable Differences in Behavior to Error Inputs”. The vulnerability cannot be fixed, only mitigations are available.

CVE-2021-3011 is assigned to this vulnerability.

2.2 CVSS Rating

The CVSS v3.1 Base Score is rated at: 4.2 (medium)
CVSS:3.1/AV:P/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

2.3 Impact

The attacker must obtain the camera physically, open the device, gain access to the security microcontroller and perform detailed analysis by physical intrusion on the chip. The equipment and knowledge for conducting side-channel attacks on the chip is necessary by the attacker.

If the attack is successful, the private key for an ECDSA certificate can be extracted from the chip.

Bosch does not include any default certificates using ECDSA keys. ECDSA keys can only be installed or generated by the customer. If no ECDSA keys are used on the device this vulnerability does not apply.

Installed ECDSA certificates may be used by the customer as:

- HTTPS certificate for the camera
- Signing Video Streams
- Network authentication (802.1X)

If different certificates are used for each camera, the attacker can only obtain the private key for a single camera.

Depending on the usage of the extracted key, an attacker would have the possibility to conduct MITM (Man in the Middle) attacks, create signed video streams or authenticate to network.

3 Vulnerability Fix

The vulnerable chip cannot be updated, no fix is available. Please use a risk-based approach and consider listed mitigations.

4 Mitigations and Workarounds

4.1 Replacing ECDSA Keys with RSA Keys

In case ECDSA keys are used on this device, new keys using RSA can be created or uploaded which are not vulnerable to this attack.

4.2 Invalidating lost keys / devices

If a device is lost or missing, the according keys should be invalidated in the according CA and certificate revocation information distributed via CRL or OCSP so an attacker cannot use these keys anymore.

4.3 Secure Disposal

When disposing the camera, a wipe of the camera should be performed before taking it out of order. A wipe (factory default) will securely delete the keys (and other sensitive data) on the device, making it impossible to recover certificates from it.

4.4 Upgrade camera model

The upcoming cameras built on CPP13 and CPP14 are not using the vulnerable chip anymore.

5 Affected Hardware

5.1 Bosch cameras and encoders

As the vulnerability is related to the built-in hardware component, there is no firmware relation. All platforms CPP-ENC, CPP3, CPP4, CPP5, CPP6, CPP7 and CPP7.3 are affected, regardless of firmware version installed (for a full list, see Appendix A).

6 Direct Links

Bosch Building Technologies Security Advisory page

Bosch PSIRT

7 Document Change Log

2020.03.03 – Revision 1.00: Initial Release

A Appendix Affected Bosch Product Families

CPP7.3

- AUTODOME IP 4000i
- AUTODOME IP 5000i
- AUTODOME IP starlight 5000i (IR)
- AUTODOME IP starlight 7000i
- DINION IP 3000i
- DINION IP bullet 4000i
- DINION IP bullet 5000
- DINION IP bullet 5000i
- DINION IP bullet 6000i
- FLEXIDOME IP 3000i
- FLEXIDOME IP 4000i
- FLEXIDOME IP 5000i
- FLEXIDOME IP starlight 5000i (IR)
- FLEXIDOME IP starlight 8000i
- MIC IP starlight 7000i
- MIC IP starlight 7100i
- MIC IP ultra 7100i
- MIC IP fusion 9000i

CPP7

- DINION IP starlight 6000
- DINION IP starlight 7000
- DINION IP thermal 8000
- FLEXIDOME IP starlight 6000
- FLEXIDOME IP starlight 7000
- DINION IP thermal 9000 RM

CPP6

- AVIOTEC IP starlight 8000
- DINION IP starlight 8000 12MP
- DINION IP ultra 8000 12MP
- DINION IP ultra 8000 12MP with C/CS mount telephoto lens
- 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
- 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

CPP5

- VIDEOJET multi 4000
- VIP-X16XF-E

CPP4

- AUTODOME IP 4000 HD
- AUTODOME IP 5000 HD
- AUTODOME IP 5000 IR
- AUTODOME 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 micro 2000 HD
- FLEXIDOME IP micro 2000 IP
- FLEXIDOME IP indoor 4000 HD
- FLEXIDOME IP indoor 4000 IR
- FLEXIDOME IP outdoor 4000 HD
- FLEXIDOME IP outdoor 4000 IR
- FLEXIDOME IP indoor 5000 HD
- FLEXIDOME IP indoor 5000 MP
- FLEXIDOME IP micro 5000 HD
- FLEXIDOME IP micro 5000 MP
- FLEXIDOME IP outdoor 5000 HD
- FLEXIDOME IP panoramic 5000
- FLEXIDOME IP outdoor 5000 MP
- 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

CPP3

- AUTODOME Easy II IP series
- AUTODOME Junior HD, Jr HD fix
- AUTODOME 700 IP IVA
- AUTODOME 800
- AUTODOME Junior 800
- VG4 AUTODOME IP series
- VG5 AUTODOME IP series
- DINION XF 720p+, NBN-921-P
- DINION XF, NBC-455-P
- DINION 2X, NBN-498-P
- FLEXIDOME XF 720p+, NDN-921-P
- FLEXIDOME XF, NDC-455-P
- FLEXIDOME 2X, NDN-498-P
- Economy Box Cameras, NBC-225 series, NBC-255 series, NTC-255-PI
- Economy Dome Cameras, NDC-225 series, NDC-255 series
- Economy HD Box Cameras, NBC-265 series, NTC-265-PI
- Economy HD Dome Cameras, NDC-265 series, NDN-265-PIO
- Extreme series EX30 IR, NEI-30 IR Imager
- Far Infra-Red camera, VOT-320
- VIP X1 XF Single-Channel H.264 Encoder
- WLAN cameras NBC-255-W and NBC-265-W
- Economic version VIP-X1XF-E
- Video Conference Dome IVA
- REG 1.5 IP and REG L2
- MIC IP PSU

CPP-ENC

- VIP-X1600-XFM4
- VJT-X20/X40XF-E
- VJT-XTCXF
- VIDEOJET decoder 3000, VJD-3000
- VIDEOJET connect 7000, VJC-7000