Security Advisory

January 2018

Meltdown / Spectre

Source:

- https://spectreattack.com
- CVE-2017-5753 and CVE-2017-5715 (Spectre)
- CVE-2017-5754 (Meltdown)

Overview

Meltdown and Spectre exploit vulnerabilities in modern processors. These hardware vulnerabilities allow programs to get access to data which is currently processed in the computer's RAM (Random Access Memory).

Under normal conditions, programs cannot read other programs data. A malicious program can exploit Meltdown and/or Spectre and get hold of data owned by other processes. This might include passwords, personal information, messages or other documents. Meltdown breaks the mechanism that keeps applications from accessing other programs allocated RAM. Spectre can trick applications into using its own memory space, thereby having also access rights to this part of the memory. The result of both vulnerabilities is the same, therefore they are typically mentioned together.

Malware exploiting these vulnerabilities would be designed to identify and read specific data. An attacker must be able to successfully install the crafted software onto the target device. It is not possible to use the vulnerability to attack a computer interface over the network. Infection with such software would typically occur when installing compromised applications, opening a compromised email attachment or possibly spread in an already infected system.

Risk assessment

Compared with a PC or mobile device, Axis cameras, speaker and access control devices do not have users that open suspicious email attachments, install user applications or browse compromised web pages. However, with administrator credentials it is possible to install add-on services (ACAP) onto an Axis device.

Axis devices do not store or process data in such a way that an attacker would profit from exploiting the Spectre vulnerability. An attacker who is able to exploit it already has the possibility to carry out more severe attacks. Spectre does not pose any additional risk compared to other potential attack vectors.

The Axis Recorder (S10/S20) is a Video Management System (VMS) running on an Intel platform with Windows. The VMS does not produce, store or processes data where Meltdown and Spectre pose a threat, however Intel processors are susceptible to Meltdown which can result in privilege escalation. Windows may store credentials and other encrypted secrets where the vulnerabilities could pose additional risks (just like other Windows PC or servers).

Axis Communications AB, Emdalavägen 14, SE-223 69 Lund, Sweden
Tel: +46 46 272 18 00, Fax: +46 46 13 61 30, www.axis.com
Vat.No. SE 556253-614301

Security Advisory

January 2018

Risk mitigation

For Axis devices, mitigate risks by following the Axis Hardening Guide. Use strong passwords and have a process/policy that reduces the risk of passwords being shared within your organization. Do not install device addons (ACAP) from untrusted sources.

Higher priority should be given to updating Intel-based S10/S20 devices with the latest Windows security patches.

- Apply the applicable operating system (OS) patch
- Apply the applicable BIOS firmware

If you have any concerns or questions regarding the above please contact AXIS Technical Support.

Affected Axis products

Axis devices based on ARM architecture are affected by the Spectre vulnerability but not Meltdown. Axis S10/S20 NVR based on Intel/Windows platform is affected by both Meltdown and Spectre.

The following devices models are based on ARM and are affected by Spectre (not Meltdown):

206,207/W/MW,209/FD/MFD/-R,211/M/W,212PTZ/-V,216FD/-V/MFD,247S,FA54,M1004-W, M1011,M1011-W,M1013,M1014,M1025,M1031-W,M1033-W,M1034-W,M1045-LW,M1065/-L/-LW, M1143-L,M1144-L,M2026-LE,M2026-LE Mk II,M3004-V,M3005-V,M3011,M3024-LVE,M3025-VE, M3044/-V/-WV,M3045/-V/-WV,M3046-V,M3047-P,M3048-P,M3106/-L/-LVE,M3106-L Mk II, M3106-LVE Mk II,P1311,P1367/-E,P1368-E,P1428-E,P3227/-LV/-LVE,P3228-LV/-LVE, P7701,Q1659,Q3517/-LV/-LVE,Q3708-PVE,Q3709-PVE,Q6128-E,Q8108-R

Unaffected Axis devices

For reference, the following Axis devices models are not based on ARM and are not affected by Meltdown nor Spectre.

205,210,211,213,221,221,230,240,262,282,2100,2110,2120,2130,2400,2401,2411,2420,2460,206M,206W,210A,211A,2130R,214PTZ,215PTZ/-E,223M,225FD,231D,231D+,232D,232D+,233D,2400+,2401+,240Q, 240QBlade,241Q,241QBlade,241QA, 241S,241S Blade, 241SA,2420,243QBlade,243SA,250S,262+,A1001, A8004-VE,A8105-E,A9161,A9188/-VE, F34,F41,F44,M1054,M1103,M1104,M1113/-E,M1113-E, M1114/-E, M1114-E,M1124/-E,M1125/-E, M1145/-L,M1145/-L,M2025-LE,M3006-V, M3007-P/-P,M3014,M3026-VE, M3027-PVE,M3037-PVE, M3104-L/-LVE,M3105-L/-LVE, M3113-R/-VE,M3114-R/-VE,M3203/-V,M3204/-V, M5013/-V, M5014/-V,M5054,M5525-E, M7001,M7010,M7011,M7014,M7016,P1204,P1214/-E,P1224-E, P1244,P1245,P1254, P1264,P1265,P1275,P1280-E,P1343/-E,P1344/-E,P1346/-E,P1347/-E, P1353/-E, P1354/-E/-Z/-ZB,P1355/-E,P1357/-E,P1364/-E,P1365/-E/MKII,P1405-E/-LE, P1425-E/-LE,P1427E/-LE, P1435-E/-LE/-LVE,P3214-V/-VE/-ZV/-ZBE,P3215-V/-VE/-ZV/-ZBE, P3224/-LV/-LVE/Mk II,P3225/-LV/-LVE/Mk II,P3301/-V, P3304/-V,P3343/-V,P3344/-V/-VE,P3346/-V/-VE,P3353,P3354,P3363-V/-VE, P3364-V/-LV/-LVE,P3365-V/-VE/-ZBV,P3367/-V-VE,P3374/-V/-LV,P3375-LV/-LVE, P3384/-V/-VE,P3707-PE,P3904-R/MK II,P3905/-R/-RE/Mk II,P3915-R/Mk II,P5414-E, P5415-E,P5512/-E,P5514/-E,P5515/-E, P5522/-E,P5532/-E,P5534/-E,P5544, P5624-E/Mk II,P5635-E/Mk II,P7210,P7214,P7216, P7224 Blade,P8513,P8514, P8524,P8535,P8804,Q1602/-V,Q1604/-E,Q1614/-E,Q1615/-E/Mk II, Q1635/-E, Q1755/-E,Q1765-LE,Q1775/-E,Q1910/-E,Q1921/-E,Q1922/-E,Q1932/-E,Q1941-E, Q1942-E,Q2901-E, Q3504-V/-VE,Q3505/-V/-VE/Mk II,Q3615-VE,Q3617-VE,Q6000-E/Mk II, Q6032-E,Q6034/-C/-E,Q6035/-E, Q6042/-C/-E/-S,Q6044/-C/-E/-E/-ZE,Q6045/-E/-C/-S/Mk II,Q6045/Mk II,Q6052/-E,Q6054/-E/Mk II, Q6055/-C/-E/-S,Q6114-E,Q6115-E,Q6124-E, Q6155-E,Q7401,Q7404,Q7411,Q7414 Blade,Q7424-R/Mk II,Q7436 Blade,Q8414-LVS,Q8631-E,Q8632-E,Q8641-E,Q8642-E,Q8665/-E/-LE,Q8721-E,Q8722-E,Q8741-E,Q8742-E,V5914,V5915

Axis Communications AB, Emdalavägen 14, SE-223 69 Lund, Sweden
Tel: +46 46 272 18 00, Fax: +46 46 13 61 30, www.axis.com
Vat.No. SE 556253-614301