Security Advisories

Cybersecurity resources | Vulnerability management | Axis Vulnerability Management Policy

About

The purpose of this registry is to proactively raise awareness and communicate about vulnerabilities that have been analyzed for Axis products and services.

- Axis and OpenSource vulnerabilities are listed below with CVE IDs (CVE = Common Vulnerabilities and Exposures).
- Axis vulnerabilities were previously listed with ACV IDs (ACV = Axis Critical Vulnerability), which changed when Axis was approved as a CVE Numbering Authority (CNA) in April 2021.

Please contact *Axis Technical Support* in case you have found a CVE that was reported to be present in AXIS OS and is not registered below.

To learn more please watch the *YouTube video* about Vulnerability Management. For more information about Axis work with cybersecurity, see *Cybersecurity resources*.

Axis CVEs

The Axis registry covers vulnerabilities that are specific to Axis products and services. We strongly recommend to update affected devices and services.

Analytics

CVE 2023

CVE number	CVSS severity	Released version	Security advisory / Vulnerability summary
CVE-2023-21412	7.2 (High)	2.8.4	*Axis Security Advisory* - AXIS License Plate Verifier: User provided input is not sanitized on the "search.cgi" allowing for SQL injections.
CVE-2023-21411	7.2 (High)	2.8.4	*Axis Security Advisory* - AXIS License Plate Verifier: User provided input is not sanitized in the "Settings > Access Control" configuration interface allowing for arbitrary code execution.
CVE-2023-21410	7.2 (High)	2.8.4	*Axis Security Advisory* - AXIS License Plate Verifier: User provided input is not sanitized on the AXIS License Plate Verifier specific "api.cgi" allowing for arbitrary code execution.
CVE-2023-21409	8.4 (High)	2.8.4	*Axis Security Advisory* - AXIS License Plate Verifier: Due to insufficient file permissions, unprivileged users could gain access to unencrypted administrator credentials allowing the configuration of the application.

CVE-2023-21408	8.4 (High)	2.8.4	*Axis Security Advisory* - AXIS License Plate Verifier: Due to insufficient file permissions, unprivileged users could gain access to unencrypted user credentials that are used in the integration interface towards 3rd party systems.
CVE-2023-21407	8.8 (High)	2.8.4	*Axis Security Advisory* - AXIS License Plate Verifier: A broken access control was found allowing for privileged escalation of the operator account to gain administrator privileges.

AXIS Camera Station

CVE 2025

CVE number	CVSS se
CVE-2025-13064	5.7 (Me(
CVE-2025-12757	4.6 (Me(
CVE-2025-12063	4.5 (Me(
CVE-2025-11547	7.8 (Hig
CVE-2025-30026	4.8 (Me(
CVE-2025-30025	4.8 (Me(
CVE-2025-30023	9.0 (Crit
CVE-2025-7622	5.1 (Me(
CVE-2025-1056	6.1 (Me(
CVE-2025-0926	5.9 (Me(

CVE 2024

CVE number	CVSS se
CVE-2024-7696	6.3 (Me
CVE-2024-6831	4.4 (Me
CVE-2024-6749	6.3 (Me
CVE-2024-6476	4.2 (Me

AXIS Device Manager

CVE 2025

CVE number	CVSS se
CVE-2025-30025	4.8 (Me
CVE-2025-30024	6.8 (Me
CVE-2025-30023	9.0 (Crit

CVE 2021

CVE number	CVSS severity	Released version	Security advisory / Vulnerability summary
CVE-2021-31989	5.3 (Medium)	5.17	*Axis Security Advisory* - A user with permission to log on to the machine hosting the AXIS Device Manager client could under certain conditions extract a memory dump from the built-in Windows Task Manager application. The memory dump may potentially contain credentials of connected Axis devices.

AXIS OS

CVE 2025

CVE number	CVSS severity	Patched version	Security advisory / Vulnerability summary
CVE-2025-30027	6.7 (Medium)	12.5.36	*Axis Security Advisory* - An ACAP configuration file lacked sufficient input validation, which could allow for arbitrary code execution.

CVE-2025-11142	7.1 (High)	12.7.53	*Axis Security Advisory* - The VAPIX API mediaclip.cgi did not have a sufficient input validation allowing for a possible remote code execution.
CVE-2025-9524	4.3 (Medium)	12.7.11 11.11.1-77 10.12.3-05 9.80.123 8.40.89 6.50.5.-21	*Axis Security Advisory* - The VAPIX API port.cgi did not have sufficient input validation, which may result in process crashes and impact usability.
CVE-2025-9055	6.4 (Medium)	12.7.53	*Axis Security Advisory* - The VAPIX Edge storage API allowed a privilege escalation, enabling a VAPIX administrator-privileged user to gain Linux Root privileges.
CVE-2025-8998	3.1 (Low)	12.7.27 11.11.1-78 10.12.3-06 9.80.124 8.40.90 6.50.5.-22	*Axis Security Advisory* - It was possible to upload files with a specific name to a temporary directory, which may result in process crashes and impact usability.
CVE-2025-8108	6.7 (Medium)	12.7.33	*Axis Security Advisory* - An ACAP configuration file had improper permissions and lacked input validation, which could potentially lead to privilege escalation.
CVE-2025-6779	6.7 (Medium)	12.6.40	*Axis Security Advisory* - An ACAP configuration file had improper permissions, which could allow command injection and potentially lead to privilege escalation.
CVE-2025-6571	6.0 (Medium)	12.6.66 11.11.1-69	*Axis Security Advisory* - A third-party component exposed its password in process arguments, allowing for low-privileged users to access it.
CVE-2025-6298	6.7 (Medium)	12.6.28	*Axis Security Advisory* - ACAP applications can gain elevated privileges due to improper input validation, potentially leading to privilege escalation.
CVE-2025-5718	6.8 (Medium)	12.6.30	*Axis Security Advisory* - The ACAP Application framework allowed a privilege escalation through a symlink attack.

CVE-2025-5454	6.4 (Medium)	12.6.18	*Axis Security Advisory* - An ACAP configuration file lacked sufficient input validation, which could allow a path traversal attack leading to potential privilege escalation.
CVE-2025-5452	6.6 (Medium)	12.6.69	*Axis Security Advisory* - A malicious ACAP application can gain access to admin-level service account credentials used by legitimate ACAP applications, leading to a potential privilege escalation of the malicious ACAP application.
CVE-2025-4645	6.7 (Medium)	12.6.7	*Axis Security Advisory* - An ACAP configuration file lacked sufficient input validation, which could allow for arbitrary code execution.
CVE-2025-3892	6.7 (Medium)	12.5.31	*Axis Security Advisory* - It was possible for ACAP applications to be executed with elevated privileges, potentially leading to privilege escalation.
CVE-2025-0361	4.3 (Medium)	12.3.56 11.11.1-41	*Axis Security Advisory* - The VAPIX Device Configuration framework allowed for unauthenticated username enumeration through the VAPIX Device Configuration SSH Management API.
CVE-2025-0360	7.8 (High)	12.2.41 11.11.1-35	*Axis Security Advisory* - The VAPIX Device Configuration framework was vulnerable to a flaw that could lead to an incorrect user privilege level in the VAPIX service account D-Bus API.
CVE-2025-0359	8.5 (High)	12.2.52 11.11.1-35	*Axis Security Advisory* - The ACAP Application framework allowed applications to access restricted D-Bus methods within the framework.
CVE-2025-0358	8.8 (High)	12.4.0	*Axis Security Advisory* - The VAPIX Device Configuration framework allowed a privilege escalation, enabling a lower-privileged user to gain administrator privileges.
CVE-2025-0325	4.3 (Medium)	12.4.28 11.11.1-42 10.12.2-78 9.80.100 8.40.74 6.50.5.-21	*Axis Security Advisory* - A Guard Tour VAPIX API parameter allowed the use of arbitrary values and can be incorrectly called, allowing an attacker to block access to the guard tour configuration page in the web interface of the Axis device.
CVE-2025-0324	9.4 (Critical)	12.3.33 11.11.1-40	*Axis Security Advisory* - The VAPIX Device Configuration framework allowed a privilege escalation, enabling a lower-privileged user to gain administrator privileges.

CVE 2024

CVE number	CVSS severity	Released version	Security advisory / Vulnerability summary
CVE-2024-47262	5.3 (Medium)	12.3.4 11.11.127 10.12.270 9.80.90 8.40.66 6.50.5.19	*Axis Security Advisory* - The VAPIX API param.cgi was vulnerable to a race condition attack allowing for an attacker to block access to the web interface of the Axis device. Other API endpoints or services not making use of param.cgi are not affected.
CVE-2024-47261	4.3 (Medium)	12.3.56 11.11.141 10.12.276	*Axis Security Advisory* - The VAPIX API uploadoverlayimage.cgi did not have sufficient input validation to allow an attacker to upload files to block access to create image overlays in the web interface of the Axis device.
CVE-2024-47260	6.5 (Medium)	12.3.1 11.11.135 10.12.270 9.80.89	*Axis Security Advisory* - The VAPIX API mediaclip.cgi did not have a sufficient input validation allowing for uploading more audio clips then designed resulting in the Axis device running out of memory.
CVE-2024-47259	3.5 (Low)	12.2.52 11.11.126	*Axis Security Advisory* - The VAPIX API dynamicoverlay.cgi did not have a sufficient input validation allowing for a possible command injection leading to being able to transfer files to the Axis device with the purpose to exhaust system resources.
CVE-2024-47257	7.5 (High)	6.50.5.19	*Axis Security Advisory* - Selected Axis devices were vulnerable to handling certain ethernet frames which could lead to the Axis device becoming unavailable in the network.
CVE-2024-8772	4.3 (Medium)	12.1.28 11.11.118 10.12.259 9.80.84	*Axis Security Advisory* - The VAPIX API managedoverlayimages.cgi was vulnerable to a race condition attack allowing for an attacker to block access to the overlay configuration page in the web interface of the Axis device.
CVE-2024-8160	3.8 (Low)	12.1.21 11.11.116 10.12.257	*Axis Security Advisory* - The VAPIX API ftptest.cgi did not have a sufficient input validation allowing for a possible command injection leading to being able to transfer files from/to the Axis device.

CVE-2024-7784	6.1 (Medium)	12.0.47 11.11.85 10.12.247	*Axis Security Advisory* - Device tampering (commonly known as Secure Boot) in AXIS OS was vulnerable to a sophisticated attack to bypass this protection. This patch will enforce a downgrade restriction. For more information please review the security advisory.
CVE-2024-6979	6.8 (Medium)	11.11.94	*Axis Security Advisory* - A broken access control was discovered which could lead to less-privileged operator- and/or viewer accounts having more privileges than designed.
CVE-2024-6509	6.5 (Medium)	11.11.93 10.12.249 9.80.78 8.40.59 6.50.5.19	*Axis Security Advisory* - The VAPIX API alwaysmulti.cgi was vulnerable for file globbing which could lead to resource exhaustion of the Axis device.
CVE-2024-6173	6.5 (Medium)	11.11.73 10.12.249 9.80.78 8.40.59 6.50.5.19	*Axis Security Advisory* - A Guard Tour VAPIX API parameter allowed the use of arbitrary values allowing for an attacker to block access to the guard tour configuration page in the web interface of the Axis device.
CVE-2024-0067	4.3 (Medium)	11.11.73 10.12.249 9.80.78 8.40.59	*Axis Security Advisory* - The VAPIX API ledlimit.cgi was vulnerable for path traversal attacks allowing to list folder/file names on the local file system of the Axis device.
CVE-2024-0066	5.3 (Medium)	11.10.61 10.12.236 9.80.69 8.40.48 6.50.5.18 5.51.7.8	*Axis Security Advisory* - A O3C feature may expose sensitive traffic between the client (Axis device) and (O3C) server. If O3C is not being used this flaw does not apply.

CVE-2024-0055	6.5 (Medium)	11.9.53 10.12.228	*Axis Security Advisory* - The VAPIX APIs mediaclip.cgi and playclip.cgi was vulnerable for file globbing which could lead to a resource exhaustion attack.
CVE-2024-0054	6.5 (Medium)	11.9.53 10.12.228 9.80.58 8.40.43 6.50.5.17	*Axis Security Advisory* - The VAPIX APIs local_list.cgi, create_overlay.cgi and irissetup.cgi was vulnerable for file globbing which could lead to a resource exhaustion attack.

CVE 2023

CVE number	CVSS severity	Released version	Security advisory / Vulnerability summary
CVE-2023-22984	6.1 (Medium)	N/A	This CVE has been rejected as it is out-of-scope in accordance with our vulnerability management policy. Please follow our general *Security Advisory about CSRF and XSS attacks* on how to mitigate these type of vulnerabilities.
CVE-2023-21418	7.1 (High)	11.7.57 10.12.213 9.80.49 8.40.37 6.50.5.15	*Axis Security Advisory* - The VAPIX API irissetup.cgi was vulnerable to path traversal attacks that allows for file deletion.
CVE-2023-21417	7.1 (High)	11.7.57 10.12.208 9.80.49	*Axis Security Advisory* - The VAPIX API manageoverlayimage.cgi was vulnerable to path traversal attacks that allows for file/folder deletion.
CVE-2023-21416	7.1 (High)	11.7.57 10.12.213	*Axis Security Advisory* - The VAPIX API dynamicoverlay.cgi was vulnerable to a Denial-of-Service attack allowing for an attacker to block access to the overlay configuration page in the web

			interface of the Axis device.
CVE-2023-21415	6.5 (Medium)	11.6.94 10.12.208 9.80.47 8.40.35 6.50.5.14	*Axis Security Advisory* - The VAPIX API overlay_del.cgi was vulnerable to path traversal attacks that allows for file deletion.
CVE-2023-21414	7.1 (High)	11.6.94 10.12.208	*Axis Security Advisory* - Device tampering (commonly known as Secure Boot) in AXIS OS was vulnerable to a sophisticated attack to bypass this protection. This patch will enforce a downgrade restriction. For more information please review the secure advisory.
CVE-2023-21413	9.1 (Critical)	11.6.94 10.12.199	*Axis Security Advisory* - The application handling service in AXIS OS was vulnerable to command injection allowing an attacker to run arbitrary code.
CVE-2023-21406	7.1 (High)	1.65.5	*Axis Security Advisory* - A heap-based buffer overflow was found in the pacsiod process which is handling the OSDP communication allowing to write outside of the allocated buffer. By appending invalid data to an OSDP message it was possible to write data beyond the heap allocated buffer. The data written outside the buffer could be used to execute arbitrary code.
CVE-2023-21405	6.5 (Medium)	11.7.12.2 11.5.54 10.12.200.1 10.12.182 1.65.5	*Axis Security Advisory* - When communicating over OSDP, a flaw was found that the OSDP message parser crashes the pacsiod process, causing a temporary unavailability of the door-controlling

			functionalities meaning that doors cannot be opened or closed.
CVE-2023-21404	4.1 (Medium)	11.4.52	*Axis Security Advisory* - A static RSA key was used to encrypt Axis-specific source code in legacy LUA-components. The encryption was applied to avoid non sensitive Axis- specific code from being easily human readable.
CVE-2023-5800	5.4 (Medium)	11.8.61 10.12.221 9.80.55 8.40.43 6.50.5.16	*Axis Security Advisory* - The VAPIX API create_overlay.cgi did not have a sufficient input validation allowing for a possible remote code execution.
CVE-2023-5677	6.3 (Medium)	5.51.7.7 6.50.5.21	*Axis Security Advisory* - The VAPIX API tcptest.cgi did not have a sufficient input validation allowing for a possible remote code execution.
CVE-2023-5553	7.6 (High)	11.7.57 10.12.213	*Axis Security Advisory* - Device tampering (commonly known as Secure Boot) in AXIS OS was vulnerable to a sophisticated attack to bypass this protection. This patch will enforce a downgrade restriction. For more information please review the secure advisory.

CVE 2021–2000

CVE number	Patched	Security advisory / Vulnerability summary
CVE-2021-31988	Yes	*Axis Security Advisory*
CVE-2021-31987	Yes	*Axis Security Advisory*
CVE-2021-31986	Yes	*Axis Security Advisory*
CVE-2018-10664	Yes	*Axis Security Advisory*
CVE-2018-10663	Yes	*Axis Security Advisory*
CVE-2018-10662	Yes	*Axis Security Advisory*

CVE-2018-10661	Yes	*Axis Security Advisory*
CVE-2018-10660	Yes	*Axis Security Advisory*
CVE-2018-10659	Yes	*Axis Security Advisory*
CVE-2018-10658	Yes	*Axis Security Advisory*
CVE-2018-9158	Yes	
CVE-2018-9157	No	Disputed. This is an intended feature/functionality.
CVE-2018-9156	No	Disputed. This is an intended feature/functionality.
CVE-2017-20050	No	This CVE has been rejected as we are lacking information on how to reproduce this vulnerability.
CVE-2017-20049	Yes	*Axis Security Advisory*
CVE-2017-20048	No	This CVE has been rejected as it is out-of-scope in accordance with our vulnerability management policy.
CVE-2017-20047	No	This CVE has been rejected as it is out-of-scope in accordance with our vulnerability management policy.
CVE-2017-20046	No	This CVE has been rejected as it is out-of-scope in accordance with our vulnerability management policy
CVE-2017-15885	Yes	
CVE-2017-12413	Yes	
CVE-2016-AXIS-0812	Yes	
CVE-2015-8258	Yes	*Axis Security Advisory*
CVE-2015-8257	Yes	*Axis Security Advisory*
CVE-2015-8256	Yes	*Axis Security Advisory*
CVE-2015-8255	Yes	*Axis Security Advisory*
CVE-2013-3543	Yes	The vulnerability has been patched to affected AMC (AXIS Media Control) in AMC 6.3.8.0.
CVE-2008-5260	Yes	The vulnerability has been patched to affected products.
CVE-2007-5214	Yes	The vulnerability has been patched to affected products.
CVE-2007-5213	Yes	
CVE-2007-5212	Yes	
CVE-2007-4930	Yes	
CVE-2007-4929	Yes	
CVE-2007-4928	Yes	
CVE-2007-4927	Yes	

CVE-2007-4926	Yes	
CVE-2007-2239	Yes	
CVE-2004-2427	Yes	
CVE-2004-2426	Yes	
CVE-2004-2425	Yes	
CVE-2004-0789	Yes	
CVE-2003-1386	Yes	
CVE-2003-0240	Yes	
CVE-2001-1543	Yes	
CVE-2000-0191	Yes	
CVE-2000-0144	Yes	

ACV

CVE number	Patched	Security advisory / Vulnerability summary
ACV-2020-100004	Yes	*Axis Security Advisory*
ACV-165813	Yes	*Axis Security Advisory*
ACV-147453	Yes	*Axis Security Advisory*
ACV-128401	Yes	*Axis Security Advisory*
ACV-120444	Yes	*Axis Security Advisory*
ACV-116267	Yes	*Axis Security Advisory*

Miscellaneous

CVE 2025

CVE number	CVSS severity	Released version	Security advisory / Vulnerability summary
CVE-2025-10714	8.4 (High)	5.6.0.0	*Axis Security Advisory* - AXIS Optimizer was vulnerable to an unquoted search path vulnerability, which could potentially lead to privilege escalation within Microsoft Windows operating system.

CVE 2022

CVE number	CVSS severity	Released version	Security advisory / Vulnerability summary
CVE-2022-23410	7.8 (High)	4.18.0	*Axis Security Advisory* - AXIS IP Utility allowed for remote code execution and local privilege escalation by the means of DLL hijacking.

OpenSource CVEs

The OpenSource registry covers potential threats caused by 3rd party vulnerabilities of OpenSource components that are used in Axis products.

Severity rating

Since 2024, we have started adding the severity level to the table below. Note that it is only added for new CVE's.

Please note that the severity ratings provided for each CVE are based on calculations and assessments made by the respective open source providers. These ratings are not specific to Axis devices and do not necessarily reflect the severity of these vulnerabilities in the context of Axis products. The severity ratings provided here are intended to give a general indication of the potential impact as determined by the broader security community. If a CVSS rating is unavailable at *www.cve.org*, we refer to the *National Vulnerability Database (NVD)* for the necessary information when available.

AXIS OS

CVE 2026

CVE number	CVSS severity	Affected	Security advisory / Vulnerability summary
CVE-2026-22796	Medium	Yes	The vulnerability is patched by upgrading to OpenSSL 3.0.19.
CVE-2026-22795	Medium	Yes	The vulnerability is patched by upgrading to OpenSSL 3.0.19.

CVE 2025

CVE number	CVSS severity	Affected	Security advisory / Vulnerability summary
CVE-2025-69421	High	Yes	The vulnerability is patched by upgrading to OpenSSL 3.0.19.
CVE-2025-69420	High	Yes	The vulnerability is patched by upgrading to OpenSSL 3.0.19.
CVE-2025-69419	High	Yes	The vulnerability is patched by upgrading to OpenSSL 3.0.19.
CVE-2025-69418	Medium	Yes	The vulnerability is patched by upgrading to OpenSSL 3.0.19.
CVE-2025-68160	Medium	Yes	The vulnerability is patched by upgrading to OpenSSL 3.0.19.
CVE-2025-66200	Medium	No	AXIS OS devices do not use the vulnerable functionality.

CVE-2025-65082	Low	No	AXIS OS devices do not use the vulnerable functionality.
CVE-2025-59775	Medium	No	AXIS OS devices do not run the Windows version of Apache.
CVE-2025-58098	Low	No	AXIS OS devices do not use the vulnerable functionality.
CVE-2025-55753	Low	No	AXIS OS devices do not use the mod_md module.
CVE-2025-55182	10.0 (Critical)	No	AXIS OS devices do not use the affected versions/ components
CVE-2025-53020	Medium	Yes	The vulnerability is patched by upgrading to Apache version 2.4.64.
CVE-2025-49812	Medium	No	AXIS OS devices do not use the “SSLEngine optional” option.
CVE-2025-49630	Low	Yes	The vulnerability is patched by upgrading to Apache version 2.4.64.
CVE-2025-26466	6.8 (Medium)	Yes	The vulnerability is patched by upgrading to OpenSSH 9.9p1
CVE-2025-26465	5.9 (Medium)	No	AXIS OS devices do not utilize the affected SSH client.
CVE-2025-23048	Medium	Yes	The vulnerability is patched by upgrading to Apache version 2.4.64.
CVE-2025-15467	High	Yes	The vulnerability is patched by upgrading to OpenSSL 3.0.19.
CVE-2025-15224	Low	Yes	The vulnerability is patched by upgrading to cURL version 8.18.0. This version will only be provided on AXIS OS 11.11 and higher. For older AXIS OS LTS tracks, support for that cURL version is currently not available as it requires OpenSSL 3.0.0 and higher.
CVE-2025-15079	Low	Yes	The vulnerability is patched by upgrading to cURL version 8.18.0. This

			version will only be provided on AXIS OS 11.11 and higher. For older AXIS OS LTS tracks, support for that cURL version is currently not available as it requires OpenSSL 3.0.0 and higher.
CVE-2025-14819	Low	Yes	The vulnerability is patched by upgrading to cURL version 8.18.0. This version will only be provided on AXIS OS 11.11 and higher. For older AXIS OS LTS tracks, support for that cURL version is currently not available as it requires OpenSSL 3.0.0 and higher.
CVE-2025-14524	Low	Yes	The vulnerability is patched by upgrading to cURL version 8.18.0. This version will only be provided on AXIS OS 11.11 and higher. For older AXIS OS LTS tracks, support for that cURL version is currently not available as it requires OpenSSL 3.0.0 and higher.
CVE-2025-14017	Medium	No	AXIS OS devices do not use the vulnerable functionality.
CVE-2025-13034	Medium	No	AXIS OS devices do not use the vulnerable functionality.

CVE 2024

CVE number	CVSS severity	Affected	Security advisory / Vulnerability summary
CVE-2024-47252	Low	No	AXIS OS devices do not use the vulnerable functionality.
CVE-2024-43394	Medium	No	AXIS OS devices do not run the Windows version of Apache.
CVE-2024-43204	Low	No	AXIS OS devices do not use the mod_proxy module.

CVE-2024-42516	Medium	Yes	The vulnerability is patched by upgrading to Apache version 2.4.64.
CVE-2024-40898	7.5 (High)	No	AXIS OS devices do not run the Windows version of Apache.
CVE-2024-40725	5.3 (Medium)	No	AXIS OS devices do not utilize the affected function.
CVE-2024-39884		No	AXIS OS devices do not utilize the affected function.
CVE-2024-39573	7.5 (High)	Yes	The vulnerability is patched by upgrading to Apache version 2.4.60.
CVE-2024-38477	7.5 (High)	Yes	The vulnerability is patched by upgrading to Apache version 2.4.60.
CVE-2024-38476	9.8 (Critical)	Yes	The vulnerability is patched by upgrading to Apache version 2.4.60.
CVE-2024-38475		Yes	The vulnerability is patched by upgrading to Apache version 2.4.60.
CVE-2024-38474	9.8 (Critical)	Yes	The vulnerability is patched by upgrading to Apache version 2.4.60.
CVE-2024-38473		Yes	The vulnerability is patched by upgrading to Apache version 2.4.60.
CVE-2024-38472		No	AXIS OS devices do not run the Windows version of Apache.
CVE-2024-36387		Yes	The vulnerability is patched by upgrading to Apache version 2.4.60.
CVE-2024-28960		No	AXIS OS Z-Wave device does not use Mbed TLS.
CVE-2024-28836		No	AXIS OS Z-Wave device does not use Mbed TLS.
CVE-2024-28755		No	AXIS OS Z-Wave device does not use Mbed TLS.
CVE-2024-27316	7.5 (High)	Yes	The vulnerability is patched by upgrading to Apache version 2.4.59.
CVE-2024-26898	7.8 (High)	No	AXIS OS devices do not use this ATA over Ethernet driver.

CVE-2024-24795		Yes	The vulnerability is patched by upgrading to Apache version 2.4.59.
CVE-2024-23775	7.5 (High)	No	AXIS OS Z-Wave device does not use Mbed TLS.
CVE-2024-23744	7.5 (High)	No	AXIS OS Z-Wave device does not use Mbed TLS.
CVE-2024-23170	5.5 (Medium)	No	AXIS OS Z-Wave device does not use Mbed TLS.
CVE-2024-22472	8.1 (High)	No	AXIS OS Z-Wave devices do not use the affected module.
CVE-2024-13176	Low	Yes	Once the versions are made available by OpenSSL, the vulnerability is patched by upgrading to: OpenSSL version 1.1.1zb - LTS 2022, LTS 2020, PSS 8.40, PSS 6.50. OpenSSL version 3.0.16 - Active track 12 and LTS 2024.
CVE-2024-9681	6.5 (Medium)	Yes	The vulnerability is patched by upgrading to cURL version 8.11.0.
CVE-2024-9143		No	AXIS OS devices do not use "exotic" curves as referred to in the OpenSSL advisory.
CVE-2024-8957	9.1 (Critical)	No	AXIS OS devices do not use the affected opensource packages and implementations.
CVE-2024-8956	7.2 (High)	No	AXIS OS devices do not use the affected opensource packages and implementations.
CVE-2024-7264	6.5 (Medium)	No	AXIS OS devices do not use the affected TLS backend.
CVE-2024-6387	8.1 (High)	Yes	The vulnerability is patched by upgrading to OpenSSH version 9.8.
CVE-2024-5535	6.5 (Medium)	Yes	The vulnerability is patched by upgrading to OpenSSL version 1.1.1za (AXIS OS 6.50, LTS 2018/

			2020/2022) and OpenSSL version 3.0.15 (LTS 2024/ active track).
CVE-2024-3094	10 (Critical)	No	AXIS OS devices are running a different XZ Utils version which is not affected.
CVE-2024-3052	7.5 (High)	No	AXIS OS Z-Wave devices use a later version that is not affected.
CVE-2024-2466		No	AXIS OS devices do not use mbedTLS.
CVE-2024-2398	8.6 (High)	Yes	The vulnerability is patched by upgrading to cURL version 8.7.1.
CVE-2024-2379		No	AXIS OS devices do not use wolfSSL.
CVE-2024-2004	3.5 (Low)	Yes	The vulnerability is patched by upgrading to cURL version 8.7.1.

CVE 2023

CVE number	Affected	Security advisory / Vulnerability summary
CVE-2023-51395	No	AXIS OS Z-Wave devices are running as controllers, not end devices.
CVE-2023-48795	Yes	The vulnerability is patched by upgrading to OpenSSH version 9.6.
CVE-2023-46446	No	AXIS OS devices do not include AsyncSSH.
CVE-2023-46445	No	AXIS OS devices do not include AsyncSSH.
CVE-2023-46219	Yes	The vulnerability is patched by upgrading to cURL version 8.5.0.
CVE-2023-46218	Yes	The vulnerability is patched by upgrading to cURL version 8.5.0.
CVE-2023-45802	Yes	The vulnerability is patched by upgrading to Apache version 2.4.58.
CVE-2023-45199	No	AXIS OS Z-Wave devices do not use MBED TLS.
CVE-2023-44487	No	AXIS OS devices use the affected library in a

		different, non-vulnerable way.
CVE-2023-43622	Yes	The vulnerability is patched by upgrading to Apache version 2.4.58.
CVE-2023-38709	Yes	The vulnerability is patched by upgrading to Apache version 2.4.59.
CVE-2023-38546	Yes	The vulnerability is patched by upgrading to cURL version 8.4.0.
CVE-2023-38545	Yes	The vulnerability is patched by upgrading to cURL version 8.4.0.
CVE-2023-38408	No	AXIS OS devices do not include the ssh-agent of OpenSSH.
CVE-2023-32001	Yes	The vulnerability ispatched by upgrading to cURL version 8.0.1.
CVE–2023–31122	No	AXIS OS devices do not use the mod_macro module.
CVE-2023-28322	Yes	The vulnerability is patched by upgrading to cURL version 8.0.1.
CVE-2023-28321	Yes	The vulnerability is patched by upgrading to cURL version 8.0.1.
CVE-2023-28320	Yes	The vulnerability is patched by upgrading to cURL version 8.0.1.
CVE-2023-28319	Yes	The vulnerability is patched by upgrading to cURL version 8.0.1.
CVE-2023-27538	Yes	The vulnerability is patched by upgrading to cURL version 8.0.1.
CVE-2023-27537	Yes	The vulnerability is patched by upgrading to cURL version 8.0.1.
CVE-2023-27536	Yes	The vulnerability is patched by upgrading to cURL version 8.0.1.
CVE-2023-27535	Yes	The vulnerability is patched by upgrading to cURL version 8.0.1.
CVE-2023-27534	Yes	The vulnerability is patched by upgrading to cURL version 8.0.1.

CVE-2023-27533	No	cURL's GSS functionality is not used on AXIS OS devices.
CVE-2023-27522	No	AXIS OS devices do not use the mod_proxy_uwsgi module.
CVE-2023-26083	No	AXIS OS devices do not use this GPU Kernel driver.
CVE-2023-25690	Yes	The vulnerability is patched by upgrading to Apache version 2.4.56.
CVE-2023-25136	Yes	AXIS OS devices are running a different OpenSSH version which is not affected.
CVE-2023-23916	Yes	The vulnerability is patched by upgrading to cURL version 7.88.1.
CVE-2023-23915	No	AXIS OS devices are running a different cURL version which is not affected.
CVE-2023-23914	No	AXIS OS devices are running a different cURL version which is not affected.
CVE-2023-6246	Yes	Only AXIS OS 11 active track is affected. The vulnerability is patched by upgrading to glibc version 2.39. Other AXIS OS LTS tracks are not affected as root-privileges are already available to the user when logging in through SSH console.
CVE-2023-5678	Yes	The vulnerability is patched by upgrading to OpenSSL version 1.1.1x (AXIS OS 6.50, LTS 2018/2020/2022) & OpenSSL version 3.0.13 on active track.
CVE-2023-4807	No	AXIS OS devices do not use Windows XMM registers.
CVE-2023-4211	No	AXIS OS devices do not use this GPU Kernel driver.
CVE-2023-3817	Yes	The vulnerability is patched by upgrading to OpenSSL version 1.1.1v.
CVE-2023-3446	Yes	The vulnerability is patched by upgrading to OpenSSL version 1.1.1v.

CVE-2023-2588	No	AXIS OS devices do not have the affected function enabled.
CVE-2023-1018	No	Through testing, the vulnerability cannot be exploited in TPM modules used by Axis devices.
CVE-2023-1017	No	Through testing, the vulnerability cannot be exploited in TPM modules used by Axis devices.
CVE-2023-0466	No	AXIS OS devices do not utilize non-default certificate policy validation
CVE-2023-0465	No	AXIS OS devices do not utilize non-default certificate policy validation
CVE-2023-0464	No	AXIS OS devices do not utilize non-default certificate policy validation
CVE-2023-0401	No	AXIS OS devices are running a different OpenSSL track which is not affected.
CVE-2023-0286	Yes	The vulnerability is patched by upgrading to OpenSSL version 1.1.1t.
CVE-2023-0217	No	AXIS OS devices are running a different OpenSSL track which is not affected.
CVE-2023-0216	No	AXIS OS devices are running a different OpenSSL track which is not affected.
CVE-2023-0215	Yes	The vulnerability is patched by upgrading to OpenSSL version 1.1.1t.

CVE 2022

CVE number	Affected	Security advisory / Vulnerability summary
CVE-2022-46152	Yes	The vulnerability is patched on the AXIS OS active track and LTS 2022. Updating is recommended.
CVE-2022-43552	No	HTTP proxy tunnel functionality is not enabled on AXIS OS devices.
CVE-2022-43551	No	cURL's HSTS functionality is not enabled on AXIS OS devices.
CVE-2022-42916	Yes	The vulnerability is patched by upgrading to cURL version 7.86.0.

CVE-2022-42915	Yes	The vulnerability is patched by upgrading to cURL version 7.86.0.
CVE-2022-42889	No	AXIS OS devices do not use the affected Apache Commons software package.
CVE-2022-42012	No	While AXIS OS devices use some of the affected functions, all of these vulnerabilities require root access to be exploited and when root access is gained, full control over the device is already established.
CVE-2022-42011	No	While AXIS OS devices use some of the affected functions, all of these vulnerabilities require root access to be exploited and when root access is gained, full control over the device is already established.
CVE-2022-42010	No	While AXIS OS devices use some of the affected functions, all of these vulnerabilities require root access to be exploited and when root access is gained, full control over the device is already established.
CVE-2022-38181	No	AXIS OS devices do not use this GPU Kernel driver.
CVE-2022-37436	Yes	The vulnerability is patched by upgrading to Apache version 2.4.55.
CVE-2022-36760	No	AXIS OS devices do not use the mod_proxy_ajp module.
CVE-2022-35260	Yes	The vulnerability is patched by upgrading to cURL version 7.86.0.
CVE-2022-35252	No	AXIS OS devices do not use the cookie-engine of cURL.
CVE-2022-32221	Yes	The vulnerability is patched by upgrading to cURL version 7.86.0.
CVE-2022-32208	No	AXIS OS devices do not have Kerberos enabled.
CVE-2022-32207	Yes	The vulnerability is patched by upgrading to cURL version 7.84.0.
CVE-2022-32206	Yes	The vulnerability is patched by upgrading to cURL version 7.84.0.
CVE-2022-32205	Yes	The vulnerability is patched by upgrading to cURL version 7.84.0.
CVE-2022-31813	No	AXIS OS devices do not utilize IP based authentication.
CVE-2022-30556	Yes	The vulnerability is patched by upgrading to Apache 2.4.54.
CVE-2022-30522	No	AXIS OS devices do not use the mod_sed module.
CVE-2022-30295	Yes	Affects AXIS P7701 Video Decoder. Other Axis devices that are running the latest AXIS OS LTS or active version do not use the uClibc or uClibc-ng library. We are currently awaiting the availability of an upstream patch to be available to judge if we can provide a service release that patches this vulnerability.
CVE-2022-30115	No	
CVE-2022-29404	Yes	The vulnerability is patched by upgrading to Apache 2.4.54.
CVE-2022-28861	Yes	This vulnerability applies to Citilog software, not a vulnerability in AXIS OS itself.

CVE-2022-28860	Yes	This vulnerability applies to Citilog software, not a vulnerability in AXIS OS itself.
CVE-2022-28615	Yes	The vulnerability is patched by upgrading to Apache 2.4.54.
CVE-2022-28614	Yes	The vulnerability is patched by upgrading to Apache 2.4.54.
CVE-2022-28330	Yes	The vulnerability is patched by upgrading to Apache 2.4.54.
CVE-2022-27782	Yes	The vulnerability is patched by upgrading to cURL 7.83.1.
CVE-2022-27781	Yes	The vulnerability is patched by upgrading to cURL 7.83.1.
CVE-2022-27780	No	
CVE-2022-27779	No	
CVE-2022-27778	No	
CVE-2022-27776	Yes	The vulnerability is patched in a timely manner on the AXIS OS active track and the LTS tracks.
CVE-2022-27775	Yes	The vulnerability is patched in a timely manner on the AXIS OS active track and the LTS tracks.
CVE-2022-27774	Yes	The vulnerability is patched in a timely manner on the AXIS OS active track and the LTS tracks.
CVE-2022-26377	No	AXIS OS devices do not use the mod_proxy_ajp module.
CVE-2022-22965	No	Not affected as JDK, Spring Cloud function and/or Apache Tomcat are not used.
CVE-2022-22963	No	Not affected as JDK, Spring Cloud function and/or Apache Tomcat are not used.
CVE-2022-23943	No	AXIS OS devices do not use the mod_sed module.
CVE-2022-22721	No	While AXIS OS devices use the core module, the command LimitXMLRequestBody is unused.
CVE-2022-22720	Yes	The vulnerability is patched by upgrading to Apache version 2.4.53.
CVE-2022-22719	No	AXIS OS devices do not use the mod_lua module.
CVE-2022-22706	No	
CVE-2022-4450	Yes	The vulnerability is patched by upgrading to OpenSSL version 1.1.1t.
CVE-2022-4304	Yes	The vulnerability is patched by upgrading to OpenSSL version 1.1.1t.
CVE-2022-4203	No	AXIS OS devices are running a different OpenSSL track which is not affected.
CVE-2022-3786	No	AXIS OS devices are running a different OpenSSL track which is not affected.
CVE-2022-3602	No	AXIS OS devices are running a different OpenSSL track which is not affected.
CVE-2022-2586	Yes	All Axis products with Linux Kernel version 4.14 and onwards are affected by this vulnerability. Axis deems the severity of these vulnerabilities as low as it requires the attacker to be authenticated.

		Only after successful authentication can this vulnerability be exploited (=local exploit). We will provide patches for the Linux Kernel LTS versions that are affected in a timely manner.
CVE-2022-2585	Yes	All Axis products with Linux Kernel version 4.14 and onwards are affected by this vulnerability. We are awaiting upstream patches for the Linux Kernel LTS versions that are affected. The vulnerability is patched already for all Axis products with Linux Kernel version 5.15 and higher and has been patched for a number of products on Linux Kernel version 4.19. Axis deems the severity of these vulnerabilities as low as it requires the attacker to be authenticated. Only after successful authentication can this vulnerability be exploited (=local exploit). We will provide patches for the Linux Kernel LTS versions that are affected in a timely manner.
CVE-2022-2274	No	AXIS OS devices are running a different OpenSSL track which is not affected.
CVE-2022-2097	No	AXIS OS devices do not use an x86 architecture.
CVE-2022-2068	No	AXIS OS devices do not use the c_rehash script.
CVE-2022-1292	No	AXIS OS devices do not use the c_rehash script.
CVE-2022-0847	No	The affected Linux Kernel 5.8 is not used, AXIS OS devices utilizes lower versions of Linux Kernel on Linux Long-Term releases.
CVE-2022-0778	Yes	The vulnerability is patched by upgrading to OpenSSL version 1.1.1n.
CVE-2022-0336	No	This vulnerability is exploitable when Active Directory (AD/ADFS) services are used, which is a functionality that is not supported in AXIS OS devices.

CVE 2021

CVE number	**Affected**	**Security advisory / Vulnerability summary**
CVE-2021-44790	No	AXIS OS devices do not use the mod_lua module.
CVE-2021-44228	No	AXIS OS products only use the *vanilla Apache webserver* and **not** Apache Log4j, which is vulnerable. A general statement for the Axis portfolio can be found *here*.
CVE-2021-44224	Yes	The vulnerability is patched by upgrading to Apache version 2.4.52.
CVE-2021-43523	Yes	Affects AXIS P7701 Video Decoder. Other Axis devices that are running the latest AXIS OS LTS or active version do not use the uClibc or uClibc-ng library. We are currently awaiting the availability of an upstream patch to be available to judgeif we can provide a service release that patches this vulnerability.

CVE-2021-42013	No	
CVE-2021-41773	No	
CVE-2021-41617	No	Not affected since the AXIS OS configuration for SSH doesn't include AuthorizedKeysCommand or AuthorizedPrincipalsCommand in its default configuration.
CVE-2021-41524	No	
CVE-2021-40438	Yes	The vulnerability is patched in AXIS OS active track and the LTS tracks
CVE-2021-40146	No	
CVE-2021-39275	Yes	The vulnerability is patched in AXIS OS active track and the LTS tracks
CVE-2021-36260	No	
CVE-2021-36160	No	
CVE-2021-34798	Yes	The vulnerability has been patched on the AXIS OS active track and the LTS tracks.
CVE-2021-33910	Yes	The vulnerability has been patched. Updating is recommended.
CVE-2021-33558	No	The affected 3rd party component backup.html, preview.html, js/log.js, log.html, email.html, online-users.html, and config.js are not used in Axis products below version 5.70 that utilize the BOA webserver. Axis products with 5.70 and higher utilize the Apache webserver where these vulnerabilities do not apply as the BOA webserver has been removed.
CVE-2021-33193	Yes	Affects AXIS OS 10.1 - 10.7. The vulnerability has been patched. Updating is recommended.
CVE-2021-32934	No	
CVE-2021-31618	No	
CVE-2021-31618	No	
CVE-2021-31618	Yes	Affects AXIS OS 10.1 - 10.6. Has been patched in AXIS OS 10.7.
CVE-2021-30641	No	
CVE-2021-29462	Yes	The vulnerability has been patched on the AXIS OS active track and the LTS tracks.
CVE-2021-29256	No	AXIS OS devices do not use this GPU Kernel driver.
CVE-2021-28664	No	AXIS OS devices do not use this GPU Kernel driver.
CVE-2021-28663	No	AXIS OS devices do not use this GPU Kernel driver.
CVE-2021-28372	No	Not affected since AXIS OS doesn't utilize the ThroughTek (TUTK) TCP/IP stack application.
CVE-2021-27365	No	AXIS OS devices do not utilize ISCSI functionality.
CVE-2021-27219	Yes	The vulnerability has been patched on the LTS tracks.
CVE-2021-27218	Yes	The vulnerability has been patched on the LTS tracks.
CVE-2021-26691	No	

CVE-2021-26690	No	
CVE-2021-25677	No	
CVE-2021-23841	No	
CVE-2021-23840	No	The vulnerability has been patched on the AXIS OS active track and the LTS tracks. Updating is recommended.
CVE-2021-23839	No	
CVE-2021-22947	Yes	The vulnerability has been patched on the AXIS OS active track and the LTS tracks.
CVE-2021-22946	Yes	The vulnerability has been patched on the AXIS OS active track and the LTS tracks.
CVE-2021-22945	No	
CVE-2021-22901	No	
CVE-2021-22898	No	
CVE-2021-22897	No	
CVE-2021-22890	No	The vulnerability has been patched on the AXIS OS active track and the LTS tracks. Updating is recommended.
CVE-2021-22876	No	
CVE-2021-21727	No	
CVE-2021-4160	Yes	The vulnerability is patched by upgrading to OpenSSL 1.1.1m.
CVE-2021-4104	No	AXIS OS products only use the *vanilla Apache webserver* and **not** Apache Log4j, which is vulnerable. A general statement for the Axis portfolio can be found *here*.
CVE-2021-4034	No	Not affected since the Polkit's (PolicyKit) pkexec component is not used.
CVE-2021-4032	No	Not affected since x86-computing architecture platform is not used in AXIS OS products. AXIS OS products utilize MIPS- and ARM-based computing architecture instead.
CVE-2021-3712	Yes	The vulnerability has been patched on the AXIS OS active track and the LTS tracks. Updating is recommended.
CVE-2021-3658	Yes	Affects AXIS OS 8.40 LTS and 9.80 LTS. The vulnerability has been patched on the LTS tracks.
CVE-2021-3450	No	
CVE-2021-3449	Yes	The vulnerability has been patched on the AXIS OS active track and the LTS tracks. Updating is recommended.

CVE 2020

CVE number	Affected	Security advisory / Vulnerability summary
CVE-2020-35452	Yes	The vulnerability has been patched on the AXIS OS active track and the LTS tracks. Updating is recommended.

CVE-2020-27738	No	
CVE-2020-27737	No	
CVE-2020-27736	No	
CVE-2020-27009	No	
CVE-2020-26558	Yes	Affects Axis body worn solution and Axis wireless cameras. The vulnerability has been patched on the AXIS OS active track and the LTS tracks.
CVE-2020-25112	No	
CVE-2020-25111	No	
CVE-2020-25110	No	
CVE-2020-25109	No	
CVE-2020-25108	No	
CVE-2020-25107	No	
CVE-2020-25066	No	
CVE-2020-24383	No	
CVE-2020-24341	No	
CVE-2020-24340	No	
CVE-2020-24339	No	
CVE-2020-24338	No	
CVE-2020-24337	No	
CVE-2020-24336	No	
CVE-2020-24335	No	
CVE-2020-24334	No	
CVE-2020-17470	No	
CVE-2020-17469	No	
CVE-2020-17468	No	
CVE-2020-17467	No	
CVE-2020-17445	No	
CVE-2020-17444	No	
CVE-2020-17443	No	
CVE-2020-17442	No	
CVE-2020-17441	No	
CVE-2020-17440	No	
CVE-2020-17439	No	
CVE-2020-17438	No	
CVE-2020-17437	No	
CVE-2020-17049	No	This vulnerability is exploitable when Microsoft Kerberos services are used,

		which is a functionality that is not supported in AXIS OS devices.
CVE-2020-15795	No	
CVE-2020-14871	No	
CVE-2020-13988	No	
CVE-2020-13987	No	
CVE-2020-13986	No	
CVE-2020-13985	No	
CVE-2020-13984	No	
CVE-2020-13950	Yes	The vulnerability has been patched on the AXIS OS active track and the LTS tracks. Updating is recommended.
CVE-2020-13938	No	
CVE-2020-13848	Yes	Concerned customers can temporarily disable the parameter Network.UPnP.Enabled in Plain config to mitigate this. The vulnerability has been patched on the AXIS OS active track and the LTS tracks.
CVE-2020-12695	No	
CVE-2020-11993	No	
CVE-2020-11984	No	
CVE-2020-11899	No	
CVE-2020-11898	No	
CVE-2020-11897	No	
CVE-2020-11896	No	
CVE-2020-11023	No	Axis deems the severity and impact of this vulnerability as low as it requires the attacker to be authenticated and no known exploits are available to negatively affect the Axis product.
CVE-2020-11022	No	Axis deems the severity and impact of this vulnerability as low as it requires the attacker to be authenticated and no known exploits are available to negatively affect the Axis product.
CVE-2020-10713	No	
CVE-2020-9770	Yes	Affects Axis body worn and wireless devices and will be patched in a timely manner on the AXIS OS active track and the LTS tracks.
CVE-2020-9490	Yes	Products with AXIS OS 10.0 or lower are **not** affected. For newer AXIS OS versions, the vulnerability has been patched on the AXIS OS active track. Updating is recommended.
CVE-2020-9308	Yes	AXIS OS devices use a different (not affected) version of libarchive or affected functions require root access to be exploited and when root access is gained, full control over the device is already established.
CVE-2020-7461	No	

CVE-2020-3120	No	
CVE-2020-3119	No	
CVE-2020-3118	No	
CVE-2020-3111	No	
CVE-2020-3110	No	
CVE-2020-1971	Yes	The vulnerability has been patched on the AXIS OS active track and the LTS tracks. Updating is recommended.
CVE-2020-1967	Yes	The vulnerability has been patched on the AXIS OS active track and the LTS tracks. Updating is recommended.
CVE-2020-1938	No	
CVE-2020-1934	No	
CVE-2020-1927	Yes	The vulnerability has been patched on the AXIS OS active track and the LTS tracks. Updating is recommended.
CVE-2020-1472	No	This vulnerability is exploited when the configuration property "server schannel" is enabled. This is not supported in AXIS OS devices, instead default settings are used which are deemed secure.

CVE 2019

CVE number	Affected	Security advisory / Vulnerability summary
CVE-2019-1000020	No	AXIS OS devices use a different (not affected) version of libarchive or affected functions require root access to be exploited and when root access is gained, full control over the device is already established.
CVE-2019-1000019	No	AXIS OS devices use a different (not affected) version of libarchive or affected functions require root access to be exploited and when root access is gained, full control over the device is already established.
CVE-2019-19221	No	AXIS OS devices use a different (not affected) version of libarchive or affected functions require root access to be exploited and when root access is gained, full control over the device is already established.
CVE-2019-17567	Yes	Affects Axis door stations/intercoms. The vulnerability has been patched. Updating is recommended.
CVE-2019-15916	Yes	Affects LTS 2016. The vulnerability has been patched. Updating is recommended.
CVE-2019-12450	Yes	Affects LTS 2018 and LTS 2016. The vulnerability has been patched.
CVE-2019-11358	Yes	Axis deems the severity and impact of this vulnerability as low as it requires the attacker to be authenticated and no known exploits are available to negatively affect the Axis product.
CVE-2019-11135	No	

CVE-2019-11091	No	
CVE-2019-10744	No	
CVE-2019-9517	Yes	The vulnerability has been patched on the AXIS OS active track and the LTS tracks. Updating is recommended.
CVE-2019-1563	No	
CVE-2019-1559	No	
CVE-2019-1551	No	
CVE-2019-1547	No	
CVE-2019-1125	No	

CVE 2018

CVE number	Affected	Security advisory / Vulnerability summary
CVE-2018-1000880	No	AXIS OS devices use a different (not affected) version of libarchive or affected functions require root access to be exploited and when root access is gained, full control over the device is already established.
CVE-2018-1000879	No	AXIS OS devices use a different (not affected) version of libarchive or affected functions require root access to be exploited and when root access is gained, full control over the device is already established.
CVE-2018-1000878	No	AXIS OS devices use a different (not affected) version of libarchive or affected functions require root access to be exploited and when root access is gained, full control over the device is already established.
CVE-2018-1000877	No	AXIS OS devices use a different (not affected) version of libarchive or affected functions require root access to be exploited and when root access is gained, full control over the device is already established.
CVE-2018-25032	Yes	The vulnerability has been patched on the AXIS OS active track and the LTS tracks.
CVE-2018-12207	No	
CVE-2018-12130	No	
CVE-2018-12127	No	
CVE-2018-12126	No	
CVE-2018-10938	No	Axis OS devices do not utilize CONFIG_NETLABEL set. Additionally, the vulnerability was fixed in 4.9.125 and AXIS OS devices uses 4.9.206.
CVE-2018-3646	No	
CVE-2018-3639	No	
CVE-2018-3620	No	

CVE-2018-3615	No	
CVE-2018-1285	No	Not affected since Apache log4net is not used in AXIS OS.

CVE 2017

CVE number	Affected	Security advisory / Vulnerability summary
CVE-2017-9833	No	The affected 3rd party component /cgi-bin/wapopen is not used in Axis products below version 5.70 that utilize the BOA webserver. Furthermore, input validation in our APIs are used which would prevent injections. Axis products with 5.70 and higher utilize the Apache webserver where these vulnerabilities do not apply as the BOA webserver has been removed.
CVE-2017-5754	No	
CVE-2017-5753	Yes	Axis has delivered patches to the affected products.
CVE-2017-5715	Yes	Axis has delivered patches to the affected products.

CVE 2016

CVE number	Affected	Security advisory / Vulnerability summary
CVE-2016-20009	No	
CVE-2016-8863	Yes	Axis has delivered patches to the affected products.
CVE-2016-7409	No	
CVE-2016-7408	No	
CVE-2016-7407	No	
CVE-2016-7406	No	
CVE-2016-6255	Yes	Axis has delivered patches to the affected products.
CVE-2016-2183	Yes	The vulnerability has been patched on the active track and the LTS tracks.
CVE-2016-2147	Yes	Axis has delivered patches to the affected products.
CVE-2016-2148	Yes	Axis has delivered patches to the affected products.

CVE 2015

CVE number	Affected	Security advisory / Vulnerability summary
CVE-2015-7547	Yes	Axis has delivered patches to the affected products.

CVE-2015-0235	Yes	Axis has delivered patches to the affected products.
CVE-2015-0204	No	

CVE 2014-1999

CVE number	Affected	Security advisory / Vulnerability summary
CVE-2014-6271	No	
CVE-2014-3566	Yes	Axis has delivered patches to the affected products.
CVE-2014-0224	Yes	Axis has delivered patches to the affected products.
CVE-2014-0160	No	
CVE-2013-0156	No	AXIS OS devices do not use Ruby on Rails.
CVE-2011-3389	No	
CVE-2009-1955	No	
CVE-2007-6750	No	
CVE-2007-6514	No	
CVE-2007-1743	No	AXIS OS devices are not affected due to their locked-down filesystem permissions.
CVE-2007-1742	No	AXIS OS devices are not affected due to their locked-down filesystem permissions.
CVE-2007-1741	No	AXIS OS devices are not affected due to their locked-down filesystem permissions.
CVE-2006-20001	No	AXIS OS devices do not use the mod_dav module.
CVE-2005-1797	No	
CVE-2005-0088	No	
CVE-2002-20001	Yes	This is a known limitation of asymmetric cryptography and is not considered relevant by Axis since the web server in Axis devices supports only 20 concurrent connections at a time, which renders the attack vector ineffective. It's recommended to use symmetric cryptography instead when connecting to Axis devices.
CVE-2002-0185	No	
CVE-1999-1412	No	
CVE-1999-1237	No	

Other vulnerabilities

This section addresses vulnerabilities and/or incidents that, while not classified as CVEs, have been investigated by Axis.

Title	Details
NPM Supply Chain Attack	Statement for the NPM Supply Chain Attack.
ONVIF / WS Discovery DDoS Attacks	Statement for ONVIF-capable devices vulnerable for DDoS exploit.
Cross-Site Request Forgery (CSRF)	Statement for Cross-Site Request Forgery in Axis products.
Exposed Axis products and their risks	Statement for exposed Axis products and their risks.

T10217090

- (M8.2)