

AXIS OS Security Advisories

AXIS OS Security Advisories

[AXIS OS Portal](#) | [AXIS OS Release Notes](#) | [AXIS OS Knowledge base](#) | [AXIS OS Hardening Guide](#) | [AXIS OS YouTube playlist](#)

AXIS OS Security Advisories

AXIS OS Security Advisories

NOTICE

New Security Advisories available!

Check our updated *Security Advisories* page for the latest list of known vulnerabilities in various Axis products.

Note: This page will be removed soon. Bookmark the new Security Advisories page to stay informed about future updates.

The AXIS OS Security Advisories transparently lists both OpenSource and Axis vulnerabilities that have been brought to our attention. The purpose of the registry is to proactively raise awareness and communicate about vulnerabilities that have been analyzed for AXIS OS products.

AXIS OS devices are either running an AXIS OS LTS, active or product specific support track.

The majority of vulnerabilities reported are the result of security scanner audits that may remark vulnerabilities on Axis products falsely. To learn more about security scanner remarks, please visit the *Axis OS Vulnerability Scanner Guide*. For more information about Axis work with cybersecurity, see *Cybersecurity resources*.

OpenSource and Axis 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.

For more information when security patches are added to AXIS OS, please visit *AXIS OS Release notes*.

AXIS OS Security Advisories

OpenSource CVEs

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.

CVE 2024

CVE number	CVSS severity	Affected	Security advisory / Vulnerability summary
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.

AXIS OS Security Advisories

OpenSource CVEs

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-2024-9143		No	AXIS OS devices do not use "exotic" curves as referred to in the OpenSSL advisory.
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.

AXIS OS Security Advisories

OpenSource CVEs

CVE 2023

CVE number	Affected	Security advisory / Vulnerability summary
<i>CVE-2023-51395</i>	No	AXIS OS Z-Wave devices are running as controllers, not end devices.
<i>CVE-2023-48795</i>	Yes	The vulnerability is patched by upgrading to OpenSSH version 9.6.
<i>CVE-2023-46446</i>	No	AXIS OS devices do not include AsyncSSH.
<i>CVE-2023-46445</i>	No	AXIS OS devices do not include AsyncSSH.
<i>CVE-2023-46219</i>	Yes	The vulnerability is patched by upgrading to cURL version 8.5.0.
<i>CVE-2023-46218</i>	Yes	The vulnerability is patched by upgrading to cURL version 8.5.0.
<i>CVE-2023-45802</i>	Yes	The vulnerability is patched by upgrading to Apache version 2.4.58.
<i>CVE-2023-45199</i>	No	AXIS OS Z-Wave devices do not use MBED TLS.
<i>CVE-2023-44487</i>	No	AXIS OS devices use the affected library in a different, non-vulnerable way.
<i>CVE-2023-43622</i>	Yes	The vulnerability is patched by upgrading to Apache version 2.4.58.
<i>CVE-2023-38709</i>	Yes	The vulnerability is patched by upgrading to Apache version 2.4.59.
<i>CVE-2023-38546</i>	Yes	The vulnerability is patched by upgrading to cURL version 8.4.0.
<i>CVE-2023-38545</i>	Yes	The vulnerability is patched by upgrading to cURL version 8.4.0.
<i>CVE-2023-38408</i>	No	AXIS OS devices do not include the ssh-agent of OpenSSH.
<i>CVE-2023-32001</i>	Yes	The vulnerability is patched by upgrading to cURL version 8.0.1.
<i>CVE-2023-31122</i>	No	AXIS OS devices do not use the mod_macro module.
<i>CVE-2023-28322</i>	Yes	The vulnerability is patched by upgrading to cURL version 8.0.1.
<i>CVE-2023-28321</i>	Yes	The vulnerability is patched by upgrading to cURL version 8.0.1.
<i>CVE-2023-28320</i>	Yes	The vulnerability is patched by upgrading to cURL version 8.0.1.
<i>CVE-2023-28319</i>	Yes	The vulnerability is patched by upgrading to cURL version 8.0.1.

AXIS OS Security Advisories

OpenSource CVEs

<i>CVE-2023-27538</i>	Yes	The vulnerability is patched by upgrading to cURL version 8.0.1.
<i>CVE-2023-27537</i>	Yes	The vulnerability is patched by upgrading to cURL version 8.0.1.
<i>CVE-2023-27536</i>	Yes	The vulnerability is patched by upgrading to cURL version 8.0.1.
<i>CVE-2023-27535</i>	Yes	The vulnerability is patched by upgrading to cURL version 8.0.1.
<i>CVE-2023-27534</i>	Yes	The vulnerability is patched by upgrading to cURL version 8.0.1.
<i>CVE-2023-27533</i>	No	cURL's GSS functionality is not used on AXIS OS devices.
<i>CVE-2023-27522</i>	No	AXIS OS devices do not use the mod_proxy_uwsgi module.
<i>CVE-2023-26083</i>	No	AXIS OS devices do not use this GPU Kernel driver.
<i>CVE-2023-25690</i>	Yes	The vulnerability is patched by upgrading to Apache version 2.4.56.
<i>CVE-2023-25136</i>	Yes	AXIS OS devices are running a different OpenSSH version which is not affected.
<i>CVE-2023-23916</i>	Yes	The vulnerability is patched by upgrading to cURL version 7.88.1.
<i>CVE-2023-23915</i>	No	AXIS OS devices are running a different cURL version which is not affected.
<i>CVE-2023-23914</i>	No	AXIS OS devices are running a different cURL version which is not affected.
<i>CVE-2023-6246</i>	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.
<i>CVE-2023-5678</i>	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.
<i>CVE-2023-4807</i>	No	AXIS OS devices do not use Windows XMM registers.
<i>CVE-2023-4211</i>	No	AXIS OS devices do not use this GPU Kernel driver.
<i>CVE-2023-3817</i>	Yes	The vulnerability is patched by upgrading to OpenSSL version 1.1.1v.

AXIS OS Security Advisories

OpenSource CVEs

<i>CVE-2023-3446</i>	Yes	The vulnerability is patched by upgrading to OpenSSL version 1.1.1v.
<i>CVE-2023-2588</i>	No	AXIS OS devices do not have the affected function enabled.
<i>CVE-2023-1018</i>	No	Through testing, the vulnerability cannot be exploited in TPM modules used by Axis devices.
<i>CVE-2023-1017</i>	No	Through testing, the vulnerability cannot be exploited in TPM modules used by Axis devices.
<i>CVE-2023-0466</i>	No	AXIS OS devices do not utilize non-default certificate policy validation
<i>CVE-2023-0465</i>	No	AXIS OS devices do not utilize non-default certificate policy validation
<i>CVE-2023-0464</i>	No	AXIS OS devices do not utilize non-default certificate policy validation
<i>CVE-2023-0401</i>	No	AXIS OS devices are running a different OpenSSL track which is not affected.
<i>CVE-2023-0286</i>	Yes	The vulnerability is patched by upgrading to OpenSSL version 1.1.1t.
<i>CVE-2023-0217</i>	No	AXIS OS devices are running a different OpenSSL track which is not affected.
<i>CVE-2023-0216</i>	No	AXIS OS devices are running a different OpenSSL track which is not affected.
<i>CVE-2023-0215</i>	Yes	The vulnerability is patched by upgrading to OpenSSL version 1.1.1t.

CVE 2022

CVE number	Af- fected	Security advisory / Vulnerability summary
<i>CVE-2022-46152</i>	Yes	The vulnerability is patched on the AXIS OS active track and LTS 2022. Updating is recommended.
<i>CVE-2022-43552</i>	No	HTTP proxy tunnel functionality is not enabled on AXIS OS devices.
<i>CVE-2022-43551</i>	No	cURL's HSTS functionality is not enabled on AXIS OS devices.
<i>CVE-2022-42916</i>	Yes	The vulnerability is patched by upgrading to cURL version 7.86.0.
<i>CVE-2022-42915</i>	Yes	The vulnerability is patched by upgrading to cURL version 7.86.0.
<i>CVE-2022-42889</i>	No	AXIS OS devices do not use the affected Apache Commons software package.

AXIS OS Security Advisories

OpenSource CVEs

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	No	AXIS OS devices do not use the mod_lua module.
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	No	AXIS OS devices do not use the mod_lua module.
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	No	AXIS OS devices do not use the ap_strcmp_match() function.
CVE-2022-28614	No	AXIS OS devices do not use the ap_rwrite() function.
CVE-2022-28330	No	AXIS OS devices do not use the mod_isapi module.
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	

AXIS OS Security Advisories

OpenSource CVEs

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 <i>LimitXMLRequestBody</i> 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.

AXIS OS Security Advisories

OpenSource CVEs

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	Af- fected	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 <i>vanilla Apache webserver</i> 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 judge if 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 <i>AuthorizedKeysCommand</i> or <i>AuthorizedPrincipalsCommand</i> 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 3 rd party component <i>backup.html</i> , <i>preview.html</i> , <i>js/log.js</i> , <i>log.html</i> , <i>email.html</i> , <i>online-users.html</i> , and <i>config.js</i> 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	

AXIS OS Security Advisories

OpenSource CVEs

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 <i>vanilla Apache webserver</i> 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) pexec 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.

AXIS OS Security Advisories

OpenSource CVEs

<i>CVE-2021-3712</i>	Yes	The vulnerability has been patched on the AXIS OS active track and the LTS tracks. Updating is recommended.
<i>CVE-2021-3658</i>	Yes	Affects AXIS OS 8.40 LTS and 9.80 LTS. The vulnerability has been patched on the LTS tracks.
<i>CVE-2021-3450</i>	No	
<i>CVE-2021-3449</i>	Yes	The vulnerability has been patched on the AXIS OS active track and the LTS tracks. Updating is recommended.

CVE 2020

CVE number	Af- fected	Security advisory / Vulnerability summary
<i>CVE-2020-35452</i>	Yes	The vulnerability has been patched on the AXIS OS active track and the LTS tracks. Updating is recommended.
<i>CVE-2020-27738</i>	No	
<i>CVE-2020-27737</i>	No	
<i>CVE-2020-27736</i>	No	
<i>CVE-2020-27009</i>	No	
<i>CVE-2020-26558</i>	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.
<i>CVE-2020-25112</i>	No	
<i>CVE-2020-25111</i>	No	
<i>CVE-2020-25110</i>	No	
<i>CVE-2020-25109</i>	No	
<i>CVE-2020-25108</i>	No	
<i>CVE-2020-25107</i>	No	
<i>CVE-2020-25066</i>	No	
<i>CVE-2020-24383</i>	No	
<i>CVE-2020-24341</i>	No	
<i>CVE-2020-24340</i>	No	
<i>CVE-2020-24339</i>	No	
<i>CVE-2020-24338</i>	No	
<i>CVE-2020-24337</i>	No	
<i>CVE-2020-24336</i>	No	
<i>CVE-2020-24335</i>	No	
<i>CVE-2020-24334</i>	No	
<i>CVE-2020-17470</i>	No	
<i>CVE-2020-17469</i>	No	
<i>CVE-2020-17468</i>	No	
<i>CVE-2020-17467</i>	No	

AXIS OS Security Advisories

OpenSource CVEs

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 <i>Network.UPnP.Enabled</i> 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	

AXIS OS Security Advisories

OpenSource CVEs

<i>CVE-2020-9770</i>	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.
<i>CVE-2020-9490</i>	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.
<i>CVE-2020-9308</i>	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.
<i>CVE-2020-7461</i>	No	
<i>CVE-2020-3120</i>	No	
<i>CVE-2020-3119</i>	No	
<i>CVE-2020-3118</i>	No	
<i>CVE-2020-3111</i>	No	
<i>CVE-2020-3110</i>	No	
<i>CVE-2020-1971</i>	Yes	The vulnerability has been patched on the AXIS OS active track and the LTS tracks. Updating is recommended.
<i>CVE-2020-1967</i>	Yes	The vulnerability has been patched on the AXIS OS active track and the LTS tracks. Updating is recommended.
<i>CVE-2020-1938</i>	No	
<i>CVE-2020-1934</i>	No	
<i>CVE-2020-1927</i>	Yes	The vulnerability has been patched on the AXIS OS active track and the LTS tracks. Updating is recommended.
<i>CVE-2020-1472</i>	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	Af- fected	Security advisory / Vulnerability summary
<i>CVE-2019-1000020</i>	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.
<i>CVE-2019-1000019</i>	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.
<i>CVE-2019-19221</i>	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.
<i>CVE-2019-17567</i>	Yes	Affects Axis door stations/intercoms. The vulnerability has been patched. Updating is recommended.

AXIS OS Security Advisories

OpenSource CVEs

<i>CVE-2019-15916</i>	Yes	Affects LTS 2016. The vulnerability has been patched. Updating is recommended.
<i>CVE-2019-12450</i>	Yes	Affects LTS 2018 and LTS 2016. The vulnerability has been patched.
<i>CVE-2019-11358</i>	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.
<i>CVE-2019-11135</i>	No	
<i>CVE-2019-11091</i>	No	
<i>CVE-2019-10744</i>	No	
<i>CVE-2019-9517</i>	Yes	The vulnerability has been patched on the AXIS OS active track and the LTS tracks. Updating is recommended.
<i>CVE-2019-1563</i>	No	
<i>CVE-2019-1559</i>	No	
<i>CVE-2019-1551</i>	No	
<i>CVE-2019-1547</i>	No	
<i>CVE-2019-1125</i>	No	

CVE 2018

CVE number	Af- fected	Security advisory / Vulnerability summary
<i>CVE-2018-1000880</i>	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.
<i>CVE-2018-1000879</i>	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.
<i>CVE-2018-1000878</i>	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.
<i>CVE-2018-1000877</i>	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.
<i>CVE-2018-25032</i>	Yes	The vulnerability has been patched on the AXIS OS active track and the LTS tracks.
<i>CVE-2018-12207</i>	No	
<i>CVE-2018-12130</i>	No	
<i>CVE-2018-12127</i>	No	
<i>CVE-2018-12126</i>	No	
<i>CVE-2018-10938</i>	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.
<i>CVE-2018-3646</i>	No	
<i>CVE-2018-3639</i>	No	

AXIS OS Security Advisories

OpenSource CVEs

<i>CVE-2018-3620</i>	No	
<i>CVE-2018-3615</i>	No	
<i>CVE-2018-1285</i>	No	Not affected since Apache log4net is not used in AXIS OS.

CVE 2017

CVE number	Af- fected	Security advisory / Vulnerability summary
<i>CVE-2017-9833</i>	No	The affected 3 rd 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.
<i>CVE-2017-5754</i>	No	
<i>CVE-2017-5753</i>	Yes	Axis has delivered patches to the affected products.
<i>CVE-2017-5715</i>	Yes	Axis has delivered patches to the affected products.

CVE 2016

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

CVE 2015

CVE number	Af- fected	Security advisory / Vulnerability summary
<i>CVE-2015-7547</i>	Yes	Axis has delivered patches to the affected products.
<i>CVE-2015-0235</i>	Yes	Axis has delivered patches to the affected products.
<i>CVE-2015-0204</i>	No	

AXIS OS Security Advisories

OpenSource CVEs

CVE 2014-1999

CVE number	Af- fected	Security advisory / Vulnerability summary
<i>CVE-2014-6271</i>	No	
<i>CVE-2014-3566</i>	Yes	Axis has delivered patches to the affected products.
<i>CVE-2014-0224</i>	Yes	Axis has delivered patches to the affected products.
<i>CVE-2014-0160</i>	No	
<i>CVE-2013-0156</i>	No	AXIS OS devices do not use Ruby on Rails.
<i>CVE-2011-3389</i>	No	
<i>CVE-2009-1955</i>	No	
<i>CVE-2007-6750</i>	No	
<i>CVE-2007-6514</i>	No	
<i>CVE-2006-20001</i>	No	AXIS OS devices do not use the mod_dav module.
<i>CVE-2005-1797</i>	No	
<i>CVE-2005-0088</i>	No	
<i>CVE-2002-20001</i>	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.
<i>CVE-2002-0185</i>	No	
<i>CVE-1999-1412</i>	No	
<i>CVE-1999-1237</i>	No	

AXIS OS Security Advisories

Axis CVEs

Axis CVEs

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

Axis CVE 2024

CVE number	Patched	Result and information
CVE-2024-8772		This CVE will be externally disclosed on 26 November 2024, more detailed information will follow at that time. Review the <i>AXIS OS Release Notes</i> for patched software versions until external disclosure.
CVE-2024-8160		This CVE will be externally disclosed on 26 November 2024, more detailed information will follow at that time. Review the <i>AXIS OS Release Notes</i> for patched software versions until external disclosure.
CVE-2024-7784	Yes	<i>Axis Security Advisory</i>
CVE-2024-6979	Yes	<i>Axis Security Advisory</i>
CVE-2024-6509	Yes	<i>Axis Security Advisory</i>
CVE-2024-6173	Yes	<i>Axis Security Advisory</i>
CVE-2024-0067	Yes	<i>Axis Security Advisory</i>
CVE-2024-0066	Yes	<i>Axis Security Advisory</i>
CVE-2024-0055	Yes	<i>Axis Security Advisory</i>
CVE-2024-0054	Yes	<i>Axis Security Advisory</i>

Axis CVE 2023

CVE number	Patched	Result and information
CVE-2023-22984	No	This CVE has been rejected as it is out-of-scope in accordance with our vulnerability management policy. Please follow our general <i>Security Advisory about CSRF and XSS attacks</i> on how to mitigate these type of vulnerabilities.
CVE-2023-21418	Yes	<i>Axis Security Advisory</i>
CVE-2023-21417	Yes	<i>Axis Security Advisory</i>
CVE-2023-21416	Yes	<i>Axis Security Advisory</i>
CVE-2023-21415	Yes	<i>Axis Security Advisory</i>
CVE-2023-21414	Yes	<i>Axis Security Advisory</i>
CVE-2023-21413	Yes	<i>Axis Security Advisory</i>
CVE-2023-21412	Yes	<i>Axis Security Advisory</i>

AXIS OS Security Advisories

Axis CVEs

CVE-2023-21411	Yes	Axis Security Advisory
CVE-2023-21410	Yes	Axis Security Advisory
CVE-2023-21409	Yes	Axis Security Advisory
CVE-2023-21408	Yes	Axis Security Advisory
CVE-2023-21407	Yes	Axis Security Advisory
CVE-2023-21406	Yes	Axis Security Advisory
CVE-2023-21405	Yes	Axis Security Advisory
CVE-2023-21404	Yes	Axis Security Advisory
CVE-2023-5800	Yes	Axis Security Advisory
CVE-2023-5677	Yes	Axis Security Advisory
CVE-2023-5553	Yes	Axis Security Advisory

Axis CVE 2022-2021

CVE number	Patched	Result and information
CVE-2022-23410	Yes	Axis Security Advisory
CVE-2021-31989	Yes	Axis Security Advisory
CVE-2021-31988	Yes	Axis Security Advisory
CVE-2021-31987	Yes	Axis Security Advisory
CVE-2021-31986	Yes	Axis Security Advisory

Axis CVE 2018

CVE number	Patched	Result and information
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.

Axis CVE 2017

CVE number	Patched	Result and information
CVE-2017-20050	No	This CVE has been rejected as we are lacking information on how to reproduce this vulnerability.

AXIS OS Security Advisories

Axis CVEs

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	

Axis CVE 2016-2013

CVE number	Patched	Result and information
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.

Axis CVE 2008-2000

CVE number	Patched	Result and information
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	

AXIS OS Security Advisories

Axis CVEs

<i>CVE-2004-0789</i>	Yes	
<i>CVE-2003-1386</i>	Yes	
<i>CVE-2003-0240</i>	Yes	
<i>CVE-2001-1543</i>	Yes	
<i>CVE-2000-0191</i>	Yes	
<i>CVE-2000-0144</i>	Yes	

ACV

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

AXIS OS Security Advisories

Other

Other

This section covers vulnerabilities that are not classified as CVEs but have been investigated by Axis.

Title	Details
<i>ONVIF / WS Discovery DDoS Attacks</i>	Statement for ONVIF-capable devices vulnerable for DDoS exploit.
<i>Cross-Site Request Forgery (CSRF)</i>	Statement for Cross-Site Request Forgery in Axis products.
<i>Exposed Axis products and their risks</i>	Statement for exposed Axis products and their risks.

