Security Advisory

CVE-2026-119618 – 2026-11-16 (v1.0)

Affected products, solutions, and services

- AXIS OS 6.50.5.10 or higher

Summary

The Apache Software Foundation released Apache HTTP Server 2.4.71 on November 11, 2026, fixing CVE-2026-119618, a CVSS 9.8 Critical remote code execution vulnerability that would allow an unauthenticated attacker to gain administrator-access to the Axis network device. To Axis' knowledge, no known exploits exist publicly as of today and Axis is not aware that this has been exploited in its network products.

Solution & Mitigation

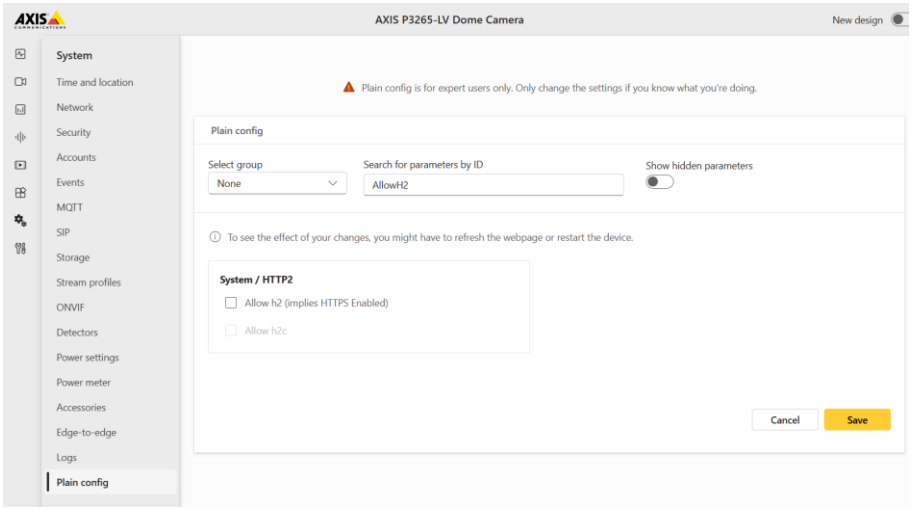
Axis is working on a service release for all affected AXIS OS tracks within the next couple of weeks, more accurate timelines will be provided in time.

The release notes will state the following:
Updated Apache to version 2.4.71 to increase overall cybersecurity.

Axis devices not included in these tracks and still under support will receive a patch according to their planned maintenance and release schedule. It is recommended to update the Axis device software. The latest Axis device software can be found here. For further assistance and questions, please contact Axis Technical Support.

As an immediate workaround, configure the Axis device as below to prevent the vulnerability exploitation. Once an update has been provided, this setting can be reverted again.

- *HTTP(S)*://<*DEVICE-IP*>/axis-cgi/param.cgi?action=update&System.HTTP2.AllowH2=no
- *HTTP(S)*://<*DEVICE-IP*>/axis-cgi/param.cgi?action=update&System.HTTP2.AllowH2c=no



Use Axis Device Manager or any other device configuration tool to mass-deploy this configuration accordingly.

Axis Vulnerability Management Portal | Axis Vulnerability Management Policy | Axis Security Notification Service

Axis Communications AB, Gränden 1, SE-223 69 Lund, Sweden
Tel: +46 46 272 18 00, Fax: +46 46 13 61 30, www.axis.com