June 11, 2026

Axis' Commitment to the EU Cyber Resilience Act

Axis is well prepared for the Cyber Resilience Act (CRA), which mandates cybersecurity standards for connected digital products to be sold within the European Union. Axis will comply with the CRA's vulnerability reporting obligations effective September 11, 2026, and will meet the product requirements that come into effect on December 11, 2027.

Axis' cybersecurity best practices align with the CRA obligations regarding essential product requirements, vulnerability handling, and user guidance. We subscribe to key principles covered by CRA: Secure by Design, Secure by Default, lifecycle management, and transparency.

Axis employs a comprehensive lifecycle approach to security, implementing rigorous measures to mitigate risks to Axis products both before and after they are sold. The Axis Security Development Model, which reflects the Secure by Design principle, guides software development to ensure security is integrated from the earliest stages of development to mitigate the risk of introducing products with exploitable vulnerabilities. Axis also implements supply chain controls to mitigate the risk of compromised components. To safeguard the integrity of Axis products, AXIS OS-based devices leverage Edge Vault features (like secure boot, signed OS, and secure storage of cryptographic keys), while our software products come with integrity checksums.

Axis products support the CRA's requirement for Secure by Default configurations. No default credentials are used. To further minimize risk out of the box, industry-standard encryption and zero-trust networking are enabled by default, while insecure protocols are disabled. In addition, our products' support for centralized identity management, audit logging, and detailed hardening guides helps customers to deploy and maintain a resilient security posture.

As a Common Vulnerabilities and Exposures Numbering Authority (CNA), Axis adheres to a vulnerability management policy for the responsible public disclosure of security incidents and newly discovered software vulnerabilities. Customers can stay informed via our notification service and receive software updates on video and device management applications from Axis and our partners. The AXIS OS platform ensures the rapid deployment of security patches and features across our extensive product portfolio, supported by management software that simplifies maintenance.

Transparency is fundamental to our operations. Beyond communicating and documenting vulnerabilities, we publish on our website a product's software bill of materials (SBOM), as well as the end of software support date that enables customers to know about a product's support lifetime before purchase.

Axis is committed to going beyond the security baselines for the physical security industry to strengthen product security and make it easier for customers to implement and maintain it. This is demonstrated through a range of measures, including bug bounty programs that help uncover vulnerabilities, automatic digital certificate management for secure operations, and resources such as the AXIS OS Vulnerability Scanner Guide and the AXIS OS Forensics Guide that assists customers in the event of a network breach.

Cybersecurity is an integral part of Axis' offerings. We remain dedicated to raising the security bar in response to an ever-evolving threat landscape.

To learn more, please visit our cybersecurity portal at www.axis.com/cybersecurity.

Jonas Falk
Director of Cybersecurity, Software Development
Axis Communications