AXIS Vulnerability Policy

September 2015

1. Overview

Axis follows industry's best practices in managing and responding to security vulnerabilities with our products to minimize customers' exposure to cyber risks. There is no way to guarantee that products and services are free from flaws which may be exploited for malicious attacks. This is not Axis-specific but a general problem for all network devices. What Axis can guarantee is that we make a devoted effort, from design to communication, to ensure the least possible risk for your Axis devices and services.

If a vulnerability flaw is detected, Axis will provide software and firmware updates as soon as possible with security fixes to customers and partners free of charge via the firmware download page www.axis.com/techsup/firmware.php – as long as the product is still supported by Axis. Security patches are always included in software/firmware releases.

Axis acknowledges that standardized network protocols and services may have weaknesses which may be exploited for attacks. While Axis cannot take responsibility for these services, we are dedicated to providing recommendations on how to reduce and eliminate risks relating to your Axis devices.

2. Reporting vulnerabilities

While Axis will work to limit risk associated with vulnerabilities, if you identify a security vulnerability with an Axis product or service, please report the problem immediately. Timely identification of security vulnerabilities is critical to eliminating potential threats.

End users, partners, vendors, industry groups and independent researchers that have identified a potential risk are encouraged to email product-security@axis.com. Please check www.axis.com/support/product-security before contacting the team as your concern may already have been processed.

Note: Axis' product security team will not process requests for support, modified features and statements. Such requests need to be sent through the appropriate Axis channel, typically sales or technical support.

Technical support: www.axis.com/techsup
General: www.axis.com

3. Response process

All valid submissions to product-security@axis.com will be processed and analyzed. Axis will reply within 48 hours with an acknowledgement and possible additional questions for investigations. Depending on severity level, Axis may follow up with posting further information on www.axis.com/support/product-security

4. Receiving Information from Axis

Axis lists vulnerability reports (CVE) and statements on **www.axis.com/support/product-security** including description, severity analysis, possible work-around, plan and credits. Please visit our website for more information.