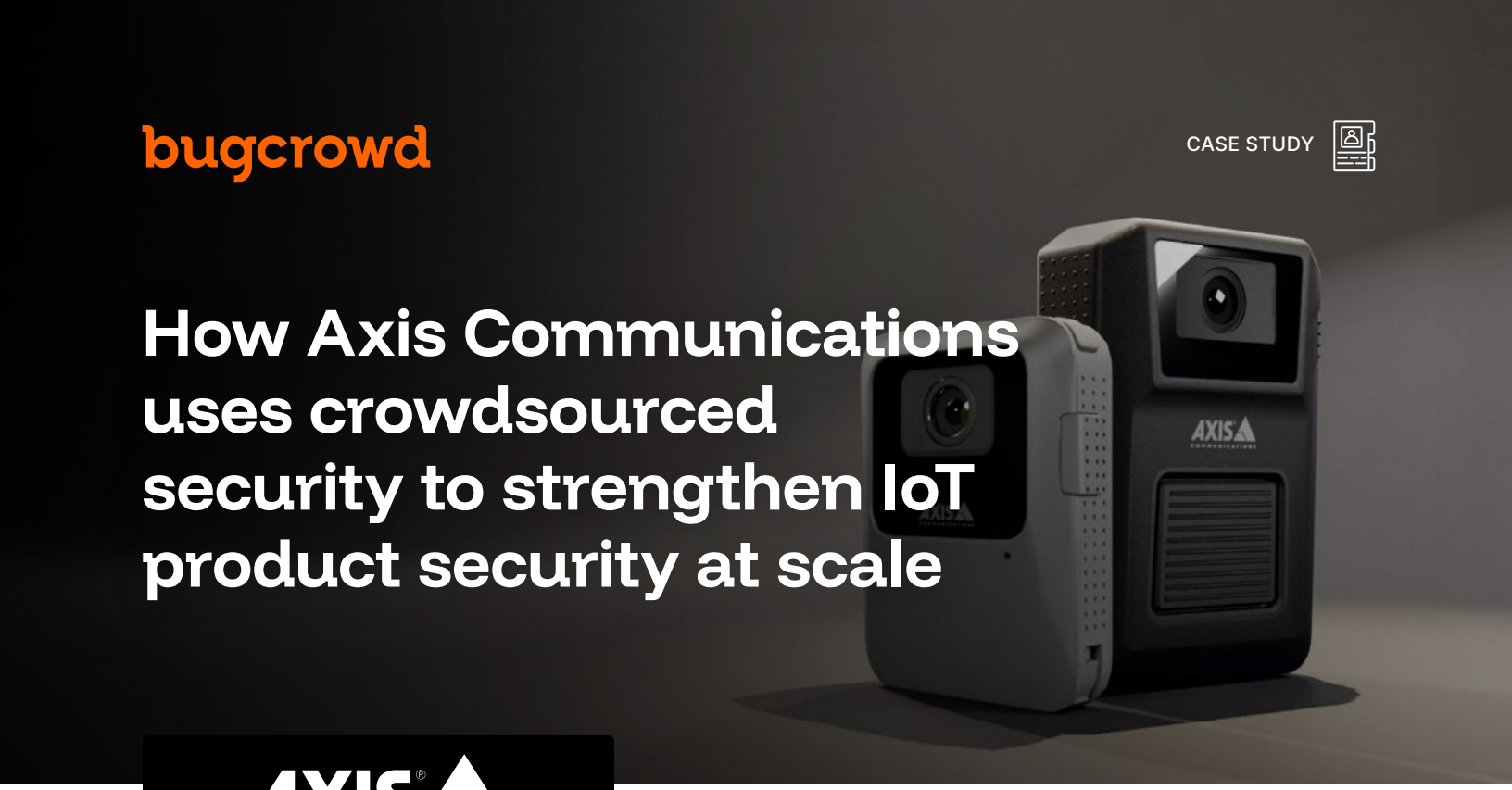
bugcrowd

CASE STUDY



How Axis Communications uses crowdsourced security to strengthen IoT product security at scale

AXIS COMMUNICATIONS

Industry:
Physical security / IoT

Founding date:
1984

Number of employees:
4K+

Headquarters:
Lund, Sweden

Website:
www.axis.com

The situation

With nearly 40 years in business, Axis Communications is an industry leader in network video surveillance and IoT solutions. Axis offers a product portfolio spanning video surveillance, access control, intercom, and audio systems that generates **$1.8 billion in revenue annually** (as of 2024).

> **The majority of their products run on AXIS OS, the company's Linux-based operating system that powers the majority of its network products and millions of devices deployed across a wide variety of installations worldwide.**

Security isn't an afterthought for Axis. As an approved Common Vulnerability and Exposures Numbering Authority (CNA), Axis is strongly committed to transparency around vulnerability management, especially since its products power critical worldwide infrastructure.

Key takeaways

More than 8,000 hackers engaged

CISA Secure by Design pledge signed in 2025

35 CVE disclosures attributed directly to bug bounty findings

Expansion from a private program to a fully public program within two years

A second program (AXIS Camera Station Pro) added alongside the AXIS OS program

The challenge

The IoT and physical security landscape is becoming a more attractive target. As device interoperability expands, attackers are broadening the attack surface and exploiting gaps that come from an integrated ecosystem.

This means that cyberattacks targeting networked physical security devices are increasing in frequency and sophistication.

Since its inception, Axis has integrated cybersecurity into its development lifecycle and worked directly with individual hackers to stress test its products. However, this approach has limits; the diversity of IoT environments and the specialized skills required to test embedded Linux devices mean that no small group of hackers can provide adequately comprehensive coverage. To stay ahead of an evolving threat environment, Axis needed a structured, scalable way to engage a broader community of hackers with **specialized IoT and device-level expertise**—without compromising the quality of its findings or the integrity of its disclosure process.

Axis decided to formalize this process by investing in a bug bounty program, connecting them with a broader community of hackers.

Essential to their decision was finding a provider that could meet specific requirements: access to a large, structured community of ethical hackers with the right expertise, and a triage process that ensured only verified, validated submissions reached the Axis team. That way, their internal security team could focus on assessing, patching, and disclosing vulnerabilities responsibly.

In an industry where customers rely on Axis products to protect physical infrastructure, maintaining customer confidence means being transparent about vulnerabilities and ensuring that when a disclosure is made, a fix is already in hand. **That standard of transparency is central to how Axis defines product security.**

The Bugcrowd solution

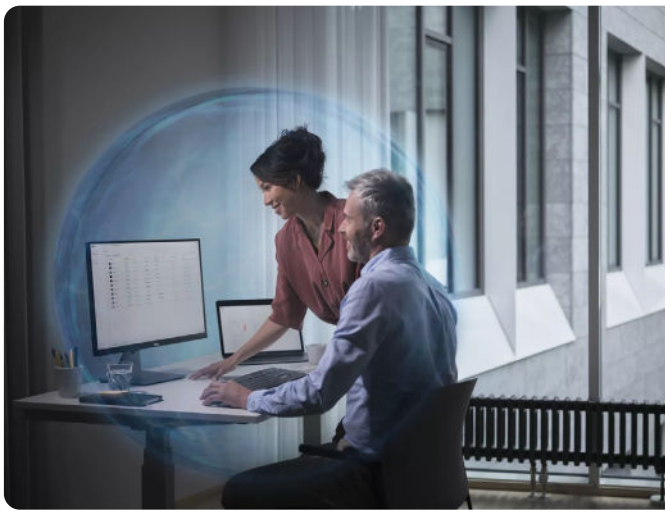
In December 2022, Axis partnered with Bugcrowd to launch a private bug bounty program, focused on AXIS OS. The program operates on a clear, transparent model: hackers identify vulnerabilities, Axis validates and patches them, and Axis then discloses them externally. Rewards are severity-based, using the Common Vulnerability Scoring System (CVSS) as the benchmark. From the outset, Axis was deliberate about making the program as accessible and rewarding as possible for the research community. **The program offers bounties up to $50,000 per validated vulnerability, plus hardware rewards for top findings.**

The Axis team didn't launch the program all at once; the controlled starting point was intentional. Bugcrowd's "crawl, walk, run" philosophy gave Axis a structured ramp-up, building program maturity before broadening access. Furthermore, Bugcrowd's CrowdMatch technology ensured that, from the outset, Axis was matched with hackers who understood IoT devices and the specific challenges of embedded systems.

> **"Engaging closely with skilled external hackers who have IoT device knowledge through our bug bounty program provides an invaluable opportunity to improve the continuous assessment of our physical security solutions," says Andre Bastert, Global Product Manager for AXIS OS.**

Feedback from hackers during the private phase led to adjustments to the program brief, the addition of swag and bonus rewards, and the inclusion of bypass rewards for vulnerabilities that had already been patched. This kept the program competitive and the hacker community engaged.

By September 2024, the program had matured enough for Axis to take a significant step forward: making the AXIS OS bug bounty program public, open to any hacker with a Bugcrowd account. Alongside this, Axis launched a new private bug bounty program for AXIS Camera Station Pro, its video management software. This extended the crowdsourced security model to another critical part of its product suite.



"Our partnership with Bugcrowd enables us to strengthen our secure development processes and ensures that our customers benefit from increased product security throughout the lifecycle," says Johan Paulsson, Chief Technology Officer at Axis Communications.

> **"This is our long-term commitment and one of the building blocks of our multi-layered approach to cybersecurity."**

The outcome

In under two years, the AXIS OS program grew from a curated private cohort to a community of more than 8,000 hackers. The results are tangible: 35 CVEs have been directly attributed to bug bounty participants.

> **Beyond the metrics, Axis has worked to establish itself as a company that the security research community genuinely wants to work with—one that treats hackers with respect, values their expertise, and is committed to deepening that relationship over time.**

Going public with the AXIS OS program signals a new level of confidence in the resilience of the operating system. In the IoT and physical security industry, where hardware vendors have historically been reluctant to invite external scrutiny, Axis's move sets a new standard for transparency.

In 2025, Axis signed the CISA Secure by Design pledge, with its Bugcrowd partnership as one of several core components of that commitment.

"Our partnership with Bugcrowd is helping to create a smarter, safer, and more cybersecure world," says Bastert. "It can feel risky at first, but working with the hacker community is one of the most effective ways to strengthen product security. Hackers bring specialized skills and fresh perspectives that complement internal testing, and a structured program creates a way to identify and address vulnerabilities responsibly before they can be exploited by threat actors."

Looking ahead, Axis plans to continue expanding its hacker community, maintain the AXIS Camera Station Pro program, and regularly review bounty reward levels to keep its programs competitive and attractive to top talent.

> Within two years, we have been disclosing more vulnerabilities than the last ten years before that, and we see this really as a success. In the end, our customers really benefit from better product security.

Andre Bastert, Global Product Manager for AXIS OS