Cyber Vulnerability Notification Procedure

PUB-CVN-001

Document Control			
Written by:	Richard Perry		
Version:	001 - 10 September 2026		
	PUBLIC		
Purpose:	Inform customers and relevant bodies		
Approved by:	Brian O'Connell	Date:	10-Sep-2026

1 How We Notify You About Security Issues

Our commitment to transparent, timely security communication under the EU Cyber Resilience Act

Active Silicon designs security in to our products from the outset. If an Actively Exploited Vulnerability[i] or Severe Incident[ii] affects a product you use, we tell you promptly, clearly, and through channels you can rely on. This page explains what you can expect from us and how to stay informed.

1.1 What we will tell you

If such a vulnerability or incident affects one of our products, our advisories tell you:

- **Which products and versions** are affected.
- **The nature of the issue** and whether it is being actively exploited.
- **What you can do right now** — workarounds or mitigations before a security update is available.
- **How to get the fix** — security updates are provided free of charge.
- **A Vulnerability Exploitability eXchange (VEX) statement** telling you whether a reported Cyber Vulnerability Event (CVE) actually affects your product where appropriate.

1.2 How quickly we act

Situation	What we do	When
A vulnerability is fixed	Publish a security advisory with the fix	At release of security update
A vulnerability is being actively exploited	Notify affected customers directly and publicly	Without undue delay
A severe security incident occurs	Notify affected customers	Without undue delay
A product approaches end-of-support	Tell you in advance so you can plan (product end-of-life procedure)	We aim for 12 months' notice

1.3 How to stay informed

Channel	What it is	For
Security notifications	https://www.activesilicon.com/support/customer-notifications/ — all our published advisories	Everyone
Email bulletin	Direct notifications to registered customers	Customers wanting alerts
Machine-readable content	CSAF 2.0 and VEX for automated ingestion where appropriate	Security & scanning tools
security.txt	activesilicon.com/.well-known/security.txt	Researchers & security teams

2 Found a security issue? Tell us

If you believe you have found a security/cyber vulnerability in an Active Silicon product, we want to hear from you.

We appreciate your vigilance and will respond to your notification within 3 working days, we do not operate a bug bounty at this moment in time.

Report a security issue: product.security@activesilicon.com
Policy & key: activesilicon.com/.well-known/security.txt
Advisories: www.activesilicon.com/support/customer-notifications/

Active Silicon Ltd complies with the vulnerability handling and reporting obligations of the EU Cyber Resilience Act (Regulation (EU) 2024/2847). This document is provided for customer information; the authoritative source of any advisory is our customer notification page.

[i] Actively Exploited Vulnerabilities: Vulnerabilities in products with digital elements that are known to be currently exploited by a malicious actor, in accordance with Article 3(42) of the CRA.

[ii] Severe Incidents: Incidents that have a severe impact on the security of the product with digital elements (e.g., compromising availability, authenticity, integrity, or confidentiality) in accordance with Article 3(44); the criteria for severity are defined in Article 14(5).