PS1012 – Security Vulnerability Disclosure Policy

Revision C

Revision Control Instructions

Post Hardcopy Revisions:	Yes
Items for Hardcopy Release:	All
Posted Locations:	CRISIS006_Product Security Incident Response Plan (PSIRP) Dropbox Folder
	External Website (https : //www.silabs.com/security)

Table of Contents:

1. Purpose

The purpose of this document is to describe the expectations and limitations regarding addressing and disclosing of security incidents related to Silicon Lab products.

2. Scope

This document applies to the following scenarios:

- Newly discovered security vulnerabilities that occur with Silicon Labs products and are not already covered in published documents/forums
- Silicon Lab collateral (documents or products) that are being used or accessed in an unexpected manner

3. Abbreviations/Definitions

- PCN – Product Change Notification
- PSIRT – Product Security Incident Response Team
- RFI – Request for Information

4. Responsibilities

- Customers, Researchers - report suspected vulnerabilities to Silicon Labs
- Sales, FAEs – gather information and related vulnerability details from the customer
- Applications – assess and confirm reproducibility related to security issue

5. Reporting Vulnerability

5.1 Vulnerability Communication

Vulnerabilities or suspicious functionality in products or software may be reported by customers, Silicon Labs employees, researchers, or other interested parties.

In addition, at least one PSIRT member will always be designated to subscribe to the CERT and CVE security feeds and constantly monitor those feeds for vulnerabilities that might affect Silicon Labs products and feed those into the PSIRT Process.

When a security vulnerability is suspected an email to be sent to product-security@silabs.com. An acknowledgement from the PSIRT will occur within 72 hours of receipt of the finding. Reporting content should include:

- The product(s) showing the vulnerability
- Product application/usage summary
- Steps and/or environment needed to reproduce/cause the issue

Further dialog on the issue will be pursued with the reporting entity by the PSIRT in a secure manner using a PGP/GPG key available at https://www.silabs.com/security/product-security.

5.2 PSIRT Process

The PSIRT works with other Silicon Labs groups including Applications, Developers, Sales and Marketing to assess reported vulnerabilities, perform technical analysis and determine an appropriate response. The key processes for addressing vulnerabilities include:

- Triage: This involves active dialog between the PSIRT and the reporting entity, Applications Support team, as well as the Engineering Design team, to determine what is needed to reproduce the vulnerability.
- Technical Analysis and Disposition: Includes the actual confirmation of the validity of the security vulnerability based on the issue's evaluation and/or reproduction. The scope and impact or severity of the

vulnerability are confirmed as well as a resolution or disposition decision. This may include a fix, work-around or acceptance of the identified vulnerability.

- Output: The level of disclosure beyond the reporting entity will depend on the severity and scope of the vulnerability.

6. Disclosure Statement

Silicon Labs intends to provide customers with the latest and accurate documentation about security related concerns associated with our products. There are multiple methods for disclosing security related updates including:

- PCNs – Product Change Notifications
- Release Notes – Documents provided with the release of software
- Direct Customer Communication – Communication through Sales or Field Application Engineers
- Security Advisories – Technical summaries about a security issue and the recommended action for addressing it

The above notification types may be signed up for at www.silabs.com under the customer profile settings.

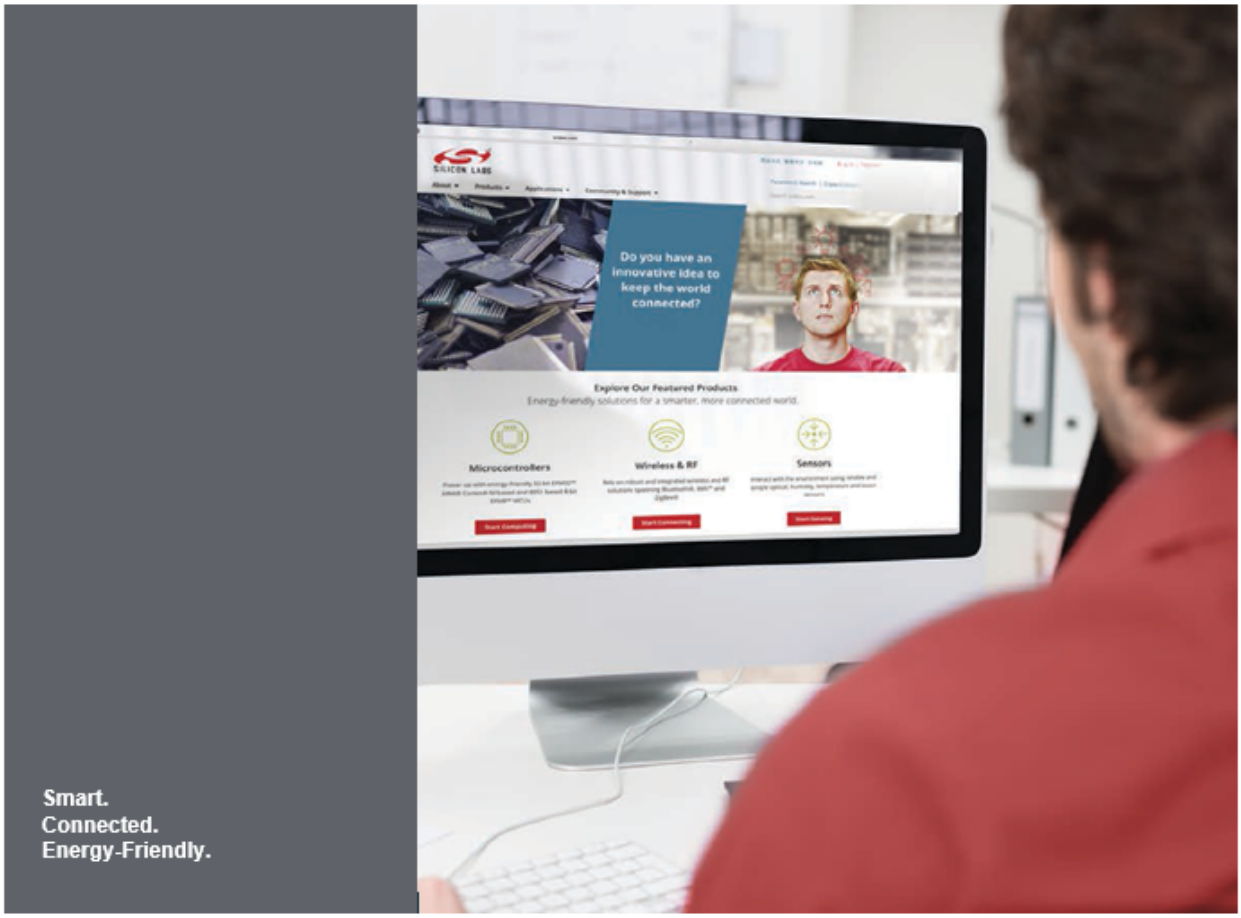
Use of products, by customers, must follow the provided specifications for operation to ensure proper functionality. In the event of a reported security concern Silicon Labs will analyze the details to assess the impact on Silicon Labs products or software, determine the associated technical cause, and provide an appropriate resolution and/or disclosure.

Silicon Labs reserves the right to adjust the (software/hardware) product if necessary for security or reliability reasons. Information sharing on vulnerabilities may take the form of release notes, PCNs, Incident Reports, Application Notes, and/or FAQs.

For details on the Terms & Conditions or product specific disclaimer content, please visit www.silabs.com. Requests for product related content not readily available at www.silabs.com may be requested through our authorized sales channel.

7. Document Revision History

Rev.	Date	Initiator	Description of Changes
A	21-Feb-2019	Esther Alexander	Initial release
B	25-Feb-2020	Esther Alexander	Added some clarifications on methods to receive security disclosures in Section 6. Disclosure Statement Added disclaimer statement on final page
C	17-Dec-2020	Esther Alexander	Added a statement on expectation regarding PSIRT subscription to CERT and CVE security feeds



Products
www.silabs.com/products

Quality
www.silabs.com/quality

Support and Community
community.silabs.com

Silicon Laboratories Inc.
400 West Cesar Chavez
Austin, TX 78701
USA

http://www.silabs.com