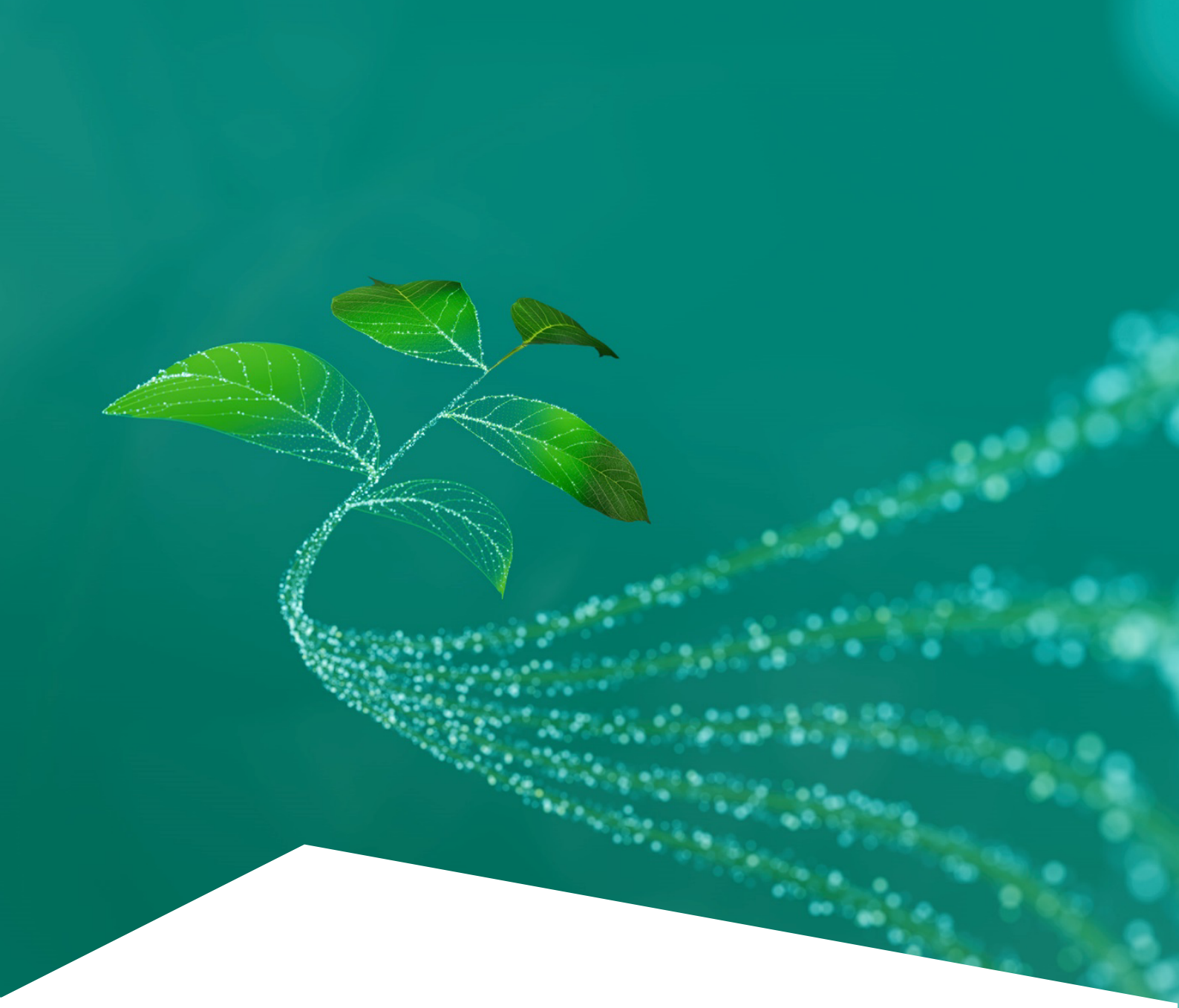

Vulnerability Notification Process

We value the contributions of the cyber security community and encourage responsible disclosure through the process described in this document.

Table of contents

1 Reporting Procedure

To report a vulnerability, please follow the steps listed below.

1. Check for eligibility in the Scope section.
2. Report details to cert@infineon.com via encrypted E-Mail, using the published Infineon Security's PGP Key available at https://www.infineon.com/cms/en/about-infineon/company/cybersecurity/.

Upon validation of a vulnerability researchers will be recognized on the Infineon Security Wall of Fame. You may choose to be listed by your full name, alias, or anonymously, and optionally include links to personal or professional social media (e.g., Twitter, LinkedIn) or hacker community profiles (e.g., Bugcrowd). Personal data provided (e.g., name, email) will be used solely for managing your recognition and communication.

Researchers can request removal from the Wall of Fame at any time by emailing cert@infineon.com with the subject "Request of removal from WoF." For more information, especially about your data subject rights, please see our Privacy Policy. (https://www.infineon.com/cms/en/about-infineon/privacy-policy/).

1.1 Prohibited Activities

- Do not attempt to harm Infineon or its users. Do not damage, destroy, or disclose data belonging to Infineon or its customers.
- Do not perform or test any (D)DoS attacks.
- Do not publicly disclose your findings until the issue is fixed.
- Do not send important data using non-encrypted channels.
- Do not publish or disclose any of Infineon's data or customer's data (in case your finding allows access to them).

1.2 Required Information

For a finding to be accepted, a report must contain at least the following minimum information:

- Textual description of the issue (clear and concise).
- Proof of Concept (code and/or screenshot).
- List of affected assets (IP and/or DNS Name).

2 Scope

This chapter describes the accepted scope for the Vulnerability Notification Process:

1. Internet-exposed systems.
2. Mobile Apps published on the App Store/Google Playstore.

2.1 Internet-Exposed Systems

In this scope are included all internet-facing assets that belong to Infineon or are managed/administrated by Infineon directly (IAAS):

- Domains: *.infineon.com, *.cypress.com, *.ifxurl.io, *.infineon.cn, *.infineon-brandportal.com, *.infineon-autoeco.com.
- Systems hosted on IPs ranges assigned to Infineon.
- Serves an SSL/TLS certificate belonging to Infineon (Cypress).
- Contains evidence that it belongs to Infineon (Cypress).

They are divided into two sub-categories:

1. IT systems and network devices (infrastructure)
2. HTTP-enabled endpoints

2.1.1 IT Systems and Network Devices

The following findings are expressly excluded from the scope:

- Usage of weak cryptography,
- Certificates/TLS/SSL related issues,
- DNS issues (i.e., MX records, SPF records),
- Exposed login screens,
- Missing brute-forcing protections,
- Best practices issues,
- Disclosure of system/technical information (i.e., software version, path disclosure, stack traces),
- Issues requiring intensive user interaction,
- Outdated/EOL products without high-security impact.

2.1.2 HTTP-Enabled EndPoints

Systems that use HTTP protocol (i.e., websites, REST APIs, WebDAV). The following findings are expressly excluded from the scope:

- Denial of service,
- Phishing,
- Fingerprinting,
- Any issue affecting only outdated browsers,
- Best practices issues,
- Disclosure of system/technical information (i.e., software version, path disclosure, stack traces),
- CSRF in forms that are available to anonymous users,
- Open redirects: we will accept reports if a high-security impact can be proven
- Clickjacking: we will accept reports if a high-security impact can be proven
- Username enumeration,
- Non-HTML content injection issues,
- Lack of Secure/HTTPOnly flags on non-security-sensitive Cookies,
- Weak Captcha/Captcha Bypass,
- Common issues with login/account creation (i.e., brute force, weak passwords, account lockout not enforced),
- Issues requiring intensive user interaction,
- Outdated/EOL products without high-security impact,
- HTTPS Mixed Content Scripts,

- Missing HTTP security headers, including:

    - Strict-Transport-Security
    - X-Frame-Options
    - X-XSS-Protection
    - X-Content-Type-Options
    - Content-Security-Policy
    - Content-Security-Policy-Report-Only

3 Document Revision History

Document Version	Release date
1.0	01.01.2021
1.1	01.01.2025

Published by
Infineon Technologies AG
Am Campeon 1-15, 85579 Neubiberg
Germany

Public

Version: V1.1_EN
Date: 04/2025

Stay connected!

Please note!
This Document is for information purposes only and any information given herein shall in no event be regarded as a warranty, guarantee or description of any functionality, conditions and/or quality of our products or any suitability for a particular purpose. With regard to the technical specifications of our products, we kindly ask you to refer to the relevant product data sheets provided by us. Our customers and their technical departments are required to evaluate the suitability of our products for the intended application.

We reserve the right to change this document and/or the information given herein at any time.

Additional information
For further information on technologies, our products, the application of our products, delivery terms and conditions and/or prices, please contact your nearest Infineon Technologies office (www.infineon.com).

Warnings
Due to technical requirements, our products may contain dangerous substances. For information on the types in question, please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by us in a written document signed by authorized representatives of Infineon Technologies, our products may not be used in any life-endangering applications, including but not limited to medical, nuclear, military, life-critical or any other applications where a failure of the product or any consequences of the use thereof can result in personal injury.

Scan QR code and explore offering
www.infineon.com