

Vulnerability Notification Process

Abstract

This document describes the Infineon Vulnerability Notification Process.

www.infineon.com v1.0

Table of contents

Abstract Table of contents		1
		2
1.1	Prohibited activities	3
1.2	Required information	3
2.1	Internet-exposed systems	4
2.1.1	IT Systems and Network Devices (infrastructure)	4
2.1.2	HTTP-enabled endpoints	4

2 2021-10 www.infineon.com

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/.

After confirming the existence of the vulnerability, contributors will be recognized on the Infineon Security Wall of Fame.

Your provided personal data (e.g., name, nickname, e-mail, phone numbers) is used exclusively for contacting you for this purpose. 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- Do not publish or disclose any of Infineon's data or customer's data (in case your finding allows access to them)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:

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

www.infineon.com

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:

- > IT systems and network devices (infrastructure)
- > HTTP-enabled endpoints

2.1.1 IT Systems and Network Devices (infrastructure)

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

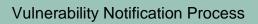
Systems that use HTTP protocol (i.e., websites, REST APIs, WebDAV). The following findings are **expressly excluded** from the scope:

- Denial of service,
- > Phishing,
- > Fingerprinting,

www.infineon.com

- 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

www.infineon.com



Published by Infineon Technologies AG 85579 Neubiberg, Germany

© 2021 Infineon Technologies AG. All Rights Reserved.