

RESPONSIBLE DISCLOSURE POLICY

IMEC VZW

Table of contents

Table of contents.....	2
1 Purpose.....	3
2 Scope.....	3
3 Responsible Disclosure Policy.....	3
3.1 Rules for Discovering Vulnerabilities.....	3
3.2 Notifying imec of a discovered vulnerability.....	4
3.3 Our Commitment.....	4
3.4 Scope Clarification.....	4

1 Purpose

At imec, we prioritize the integrity and security of our data and systems, as well as those of our partners and customers. Even though we dedicate care and attention to information security throughout our processes, a vulnerability still might be present.

Imec allows the conducting of security tests to identify potential vulnerabilities, within the limits indicated throughout its Responsible Disclosure Policy. The goals of these tests should remain to identify vulnerabilities and share this information with imec.

Should you discover a security vulnerability on one of our systems, we would love to hear about it so we can take the necessary remediation actions as soon as possible to enhance the protection of our stakeholders and systems.

Therefore, imec opts for a policy of coordinated disclosure of vulnerabilities (also known as a 'Responsible Disclosure Policy'), so that you can inform us when you'd discover a vulnerability and imec can address it in a structured and effective manner.

2 Scope

This responsible disclosure policy applies to all imec systems, with exemptions of the IP addresses or domains listed in Annex A. If you have any doubt, please reach out to responsibledisclosure@imec.be for more information.

3 Responsible Disclosure Policy

3.1 Rules for Discovering Vulnerabilities

When performing security research on our environment, certain used techniques mimic real-life attacks, and may impact our day-to-day business operations.

- The use of the following attack techniques or methods is explicitly prohibited:
 - attacks against the physical security of our imec offices or devices
 - all forms of social engineering (including phishing)
 - distributed denial of service, brute force, or other traffic-heavy attacks
 - Automated scanning tools can be used but should be throttled to limit the number of requests/second to avoid DoS-like scenarios.
 - introducing malicious code or software into imec environments (such as malware, viruses, worms, or Trojan horses).
- Do not take advantage of the vulnerability or problem you have discovered, for example, by downloading more data than necessary to demonstrate the vulnerability or by deleting, copying, or modifying imec data.
- Do not modify (the configuration of) one or more systems managed by imec nor perform simulated attacks on systems or partners of imec.
- Do not repeatedly gain access to imec data or systems or share this access with other unauthorized individuals.
- Remove all imec data that was acquired during the testing, immediately after notifying imec.

- Not to perform any actions that could impact the correct functioning of the system, both in terms of confidentiality & integrity of data as well as the availability and performance of the system.

3.2 Notifying imec of a discovered vulnerability

- If you discover a vulnerability in a system managed by imec, please do the following:
- E-mail your findings as soon as possible and exclusively to responsibledisclosure@imec.be
- Provide us with sufficient information to reproduce the problem. This will allow us to be able to resolve it as quickly as possible. Usually, the IP address or the URL of the affected system and a description of the vulnerability will be sufficient, but complex vulnerabilities may require additional information and/or further explanation.
- Leave your contact details so imec employees can contact you to work together on a secure solution. Please leave your name, email address and/or telephone number. Reporting under a pseudonym is possible, though make sure that we can contact you if we have additional questions and are able to express our appreciation for your notification.
- Acknowledge that you have acted in accordance with this policy and will continue to do so.
- Do not disclose/reveal the problem to others until it has been resolved. If you wish to publicize an article, report, blog post, etc., on the discovered vulnerability, we request you to inform us at least 30 days prior to the publication, with the possibility to respond. Refrain from including or referring to the imec brand name and/or imec-associated branding when disclosing the vulnerability publicly, unless with explicit, written consent by imec.

3.3 Our Commitment

- We commit to responding to your notification within 5 business days with our evaluation of the report and an expected resolution date and will keep you informed throughout the resolution.
- If you have followed the requirements listed in the responsible disclosure policy, and not committed other infractions, we will not take any legal action against you regarding the report.
- We will handle your report with strict confidentiality, and not pass on your personal details to third parties without your permission.
- We strive to resolve all problems as quickly as possible, though we may need to prioritize the resolution of certain vulnerabilities over others based on risk or required resources.

This text is a derivative work of "Responsible Disclosure" by Floor Terra, used under a Creative Commons Attribution license 3.0.

3.4 Scope Clarification

The following IP addresses or domains are considered out of scope of the responsible disclosure policy, as they are not under the responsibility nor the scope of influence of imec.

Value	Type
ibbt.be	Domain
iminds.be	Domain
myminds.be	Domain
robocure.be	Domain
www.fed4fire.eu	Domain
193.190.127.128/25	IP
193.190.71.128/26	IP
193.191.148.0/24	IP
193.191.169.0/24	IP
2001:6a8:1d80:1010::223	IP
2001:6a8:1d80:26::202	IP
2001:6a8:1d80:26::203	IP