Disclosure Policy

Current version: v1.0, last changed on October 17, 2023, 14.40

This policy governs the process adopted by 0xbro for reporting and disclosing vulnerabilities to product or security vendors, customers, developers, and the general public.

0xbro will **always** attempt to coordinate all reported vulnerabilities with the affected parties following a coordinated vulnerability disclosure process (also known as responsible disclosure process).

Coordinated disclosure is the most effective approach to address vulnerabilities and ensure the protection of customers. Despite this, the affected parties frequently exhibit deliberate negligence, excessive delays in developing necessary fixes, or lack of transparency towards vulnerability reports submitted them, leaving customers exposed for an irresponsible amount of time.

For this reason, **0xbro may disclose vulnerabilities to the general public fifteen (15) days after the last contact attempt without response** (see process below). **Depending on the circumstances**, including active exploitation, significant or minor threats, or the need to modify an existing standard, **the timing of disclosure may be adjusted either earlier or later**.

Disclosure process:

1. The **first contact attempt** will be through any formal mechanisms listed on the affected party web site (eg. an explicit security contact, contacts inside `/.well-known/security.txt`, etc.), or by sending an e-mail to security@, support@, info@, and secure@company.com requesting information about a security referent and a secure channel over which disclosing the technical vulnerability details. 0xbro will **never** provide information or insights about the vulnerability during this stage.
2. **If the first attempt is not followed by a response within seven (7) days**, a message requesting the security contact e-mail address may initially be sent to certain public contacts associated with the affected party (eg. public forms, general e-mails, social media, etc.) in what is considered a **second contact attempt**. Also in this case, 0xbro will **never** provide information or insights about the vulnerability during this stage..
3. **If the second attempt is not followed by a response within seven (7) days, the disclosure dates is set fifteen (15) days later.**
4. **If the involved party response is received within the fourteen (7+7) days timeframe** outlined above, 0xbro will **send a report** with the vulnerability details and some potential mitigation or workarounds. From this moment, **the involved party has thirty (30) days to address the vulnerability** with a security patch or other corrective measure as appropriate. Extensions to the 30-day disclosure timeline ***may*** be granted depending on the complexity and the effort spent to fix the flaw.
5. **If no response has been received after the 30-day disclosure timeline, the vulnerability is published immediately without further coordination attempts.**
6. **During the vulnerability analysis and remediation period**, 0xbro expects **regular updates** about the ongoing activities and is willing to cooperate appropriately for solving the problem and conducting appropriate retests. If no updates are provided by default, the **affected party will be contacted about once a week** with a status update request.

7. **If no response has been received after two (2) consecutive status update requests, no extension of the disclosure date shall be granted and the same rule as in 5th point applies.**

Vulnerabilities are disclosed to the public under these three circumstances:

- The pre-set/agreed disclosure date is reached.
- The involved party issues a fix and/or other corrective measure.
- Information about the same vulnerability is published by a third party.

Under **no circumstances** will a vulnerability that has been discovered **be suppressed or kept undisclosed** due to the unwillingness of an involved party to address it. Delays (not exceeding 15 days) to the disclosure date can be agreed upon following a fix to give customers time to install the appropriate patches.

In respect of the researcher and the time invested, the affected party is strongly encouraged to appropriately **acknowledge** and **give credit** to the reporter who submitted the issue.

If you have any questions about this policy, please contact me.