National Test Institute for Cybersecurity

NTC Vulnerability Disclosure Policy (VDP)

The NTC Vulnerability Disclosure Policy applies to vulnerabilities discovered during security tests initiated by the NTC ("Initiative Projects")

Version 1.2, 14. December 2023

Content

1 Purpose

The purpose of disclosing vulnerabilities detected by the NTC is threefold:

1. Initial private disclosure to the vendor in order to ensure a timely and correct remediation of the vulnerabilities to protect the affected systems.

2. Public disclosure of information about patterns of vulnerabilities to ensure they do not recur.

3. Public disclosure as a warning of security vulnerabilities to enable users to take their own precautions, especially when patches are not made available or delayed by vendors.

Depending on the nature of the vulnerability and the behavior of the vendor, the emphasis of the public disclosure may be on either 2) or 3) or both objectives.

2 90+30 Policy

The NTC follows a 90+30-day public disclosure policy. The public disclosure process consists of multiple steps:

2.1 Step 1: Private Disclosure

The NTC first informs only the vendor about a vulnerability. Vendors have up to 90 days after the NTC notifies them about a vulnerability to fix it, for example by providing a patch.

If a vendor is unable or unwilling to fix a vulnerability within the first 90 days, the NTC may notify the Swiss National Cyber Security Center NCSC, the Federal Data Protection and Information Commissioner FDPIC or similar governmental agencies or issue a public alert about the vulnerability including sufficient details to enable affected third parties to take appropriate protective measures. The same applies if a vendor cannot be contacted or ignores the NTC notification.

2.2 Step 2: Patch Adoption

If affected third parties are required to take any action to protect themselves (i.e. install a patch, make configuration changes, etc.), the NTC will grant an additional 30 days after the vendor fixes the issue to give them enough time to take the necessary protective measures.

If a vendor can fix a vulnerability without requiring any action by affected third parties, the NTC may publish its details as soon as it receives evidence that the vulnerability has been fixed.

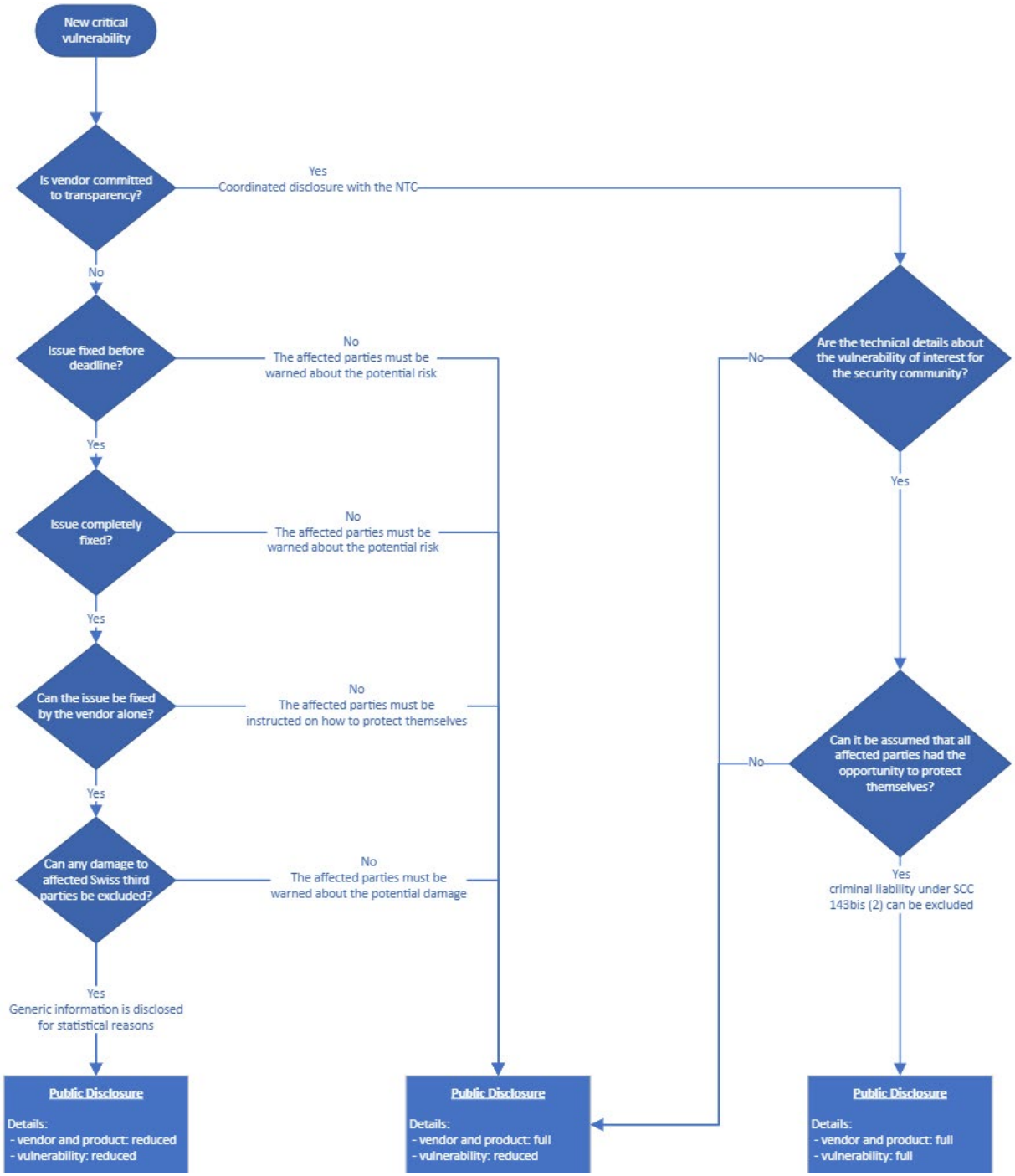
2.3 Step 3: Public Disclosure

Once the disclosure deadline has expired, the NTC will publicly disclose the vulnerability. The level of detail will vary depending on the circumstances, the nature of the vulnerability and the vendor's response. The possible levels of detail are:

- Vendor and Product Name
  - Reduced: no details about the vendor and the affected product are disclosed. Only high-level information such as the industry, geographical region, product type, etc. that may be relevant for statistical publications is included in the publication.
  - Full: the full name of the vendor and the affected product are disclosed to allow third parties to find out if they are affected.

- Vulnerability
  - Reduced: no technical details about the vulnerability are disclosed. Only high-level information such as vulnerability type, criticality, ease of exploit, etc. that may be relevant for statistical publications is included in the publication.
  - Full: the full technical details of the vulnerability are disclosed and may include a proof-of-concept exploit.

The level of detail of the public disclosure is defined based on the following decision tree:



Depending on the circumstances of the individual case, for example if there is reasonable doubt that affected parties have not been able to adequately protect themselves, the NTC may reduce the level of detail of the publication. Alternatively, the NTC may decide to notify the Swiss National Cyber Security Center NCSC about the vulnerability.

3 Grace Period

If a vendor is unable to fix a vulnerability within 90 days, but intends to fix it within a reasonable time thereafter, the NTC will, upon request, provide the vendor with an additional 14 days (i.e. within 104 days of the vulnerability being disclosed to the vendor). In this case, the NTC may still alert the public about the vulnerability and provide sufficient details to enable users to take appropriate protective measures 120 days after the vulnerability was first disclosed to the vendor.

4 In-the-wild Vulnerabilities

If the NTC finds evidence that a vulnerability is being actively exploited against real users "in the wild", a 7-day policy replaces the 90-day policy to fix the issue and the grace period is reduced to 3 days. The 30-day patch adoption window still applies if a fix is made available within the first 7 days.

5 Mutually agreed Early Disclosure

In any of the above cases, the NTC and the vendor can mutually agree to release details of a vulnerability earlier than the date indicated in this policy.

6 Frequently Asked Questions FAQ

For more information and background on this policy, please see the NTC Vulnerability Disclosure Policy FAQ.