Nationales Testinstitut
für Cybersicherheit

NTC Vulnerability Disclosure Policy (VDP)

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

Version 1.1, 7. August 2023

Table of Contents

1. Purpose

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

1. Initial private disclosure to the vendor 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 days disclosure deadline policy, which means that the NTC first informs only the vendor about a vulnerability (private disclosure). Vendors have 90 days after the NTC notifies them about a vulnerability to make a patch available to users. If they make a patch available within 90 days, the NTC will publicly disclose details of the vulnerability at the earliest 30 days after the patch has been made available to users.

For example:

- If a vendor patches a security issue 5 days after the NTC notified the vendor about the vulnerability, details would be made public not earlier than on day thirty-five.

- If a vendor patches a security issue 83 days after the NTC notified the vendor about the vulnerability, details would be made public not earlier than on day 113.

If a vendor can mitigate a vulnerability without releasing a patch to users, the NTC may publish its findings as soon as it receives evidence that the vulnerability has been fixed.

If a vendor is unable or unwilling to patch an issue 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 users to take appropriate protective measures. The same applies if a vendor cannot be contacted or ignores the NTC's notification.

3. Grace Period

If a vendor is unable to provide a patch within 90 days but intends to provide a patch 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 for the release of a patch and the grace period is reduced to 3 days. The 30-day window for the publication after the release of a patch still applies if a patch is made available within the first 7 days.

5. Level of Detail

30 days after a patch is made available, the NTC will publish the full technical details of the vulnerability, provided it is reasonable to assume that all affected parties have had an opportunity to protect

themselves. The details for publication may include a proof-of-concept exploit.

If there is reasonable doubt that affected parties have not been able to adequately protect themselves, the level of detail of the disclosure will be reduced, i.e., only partial, or full technical details about the vulnerability without a proof-of-concept exploit will be published. Alternatively, the NTC may opt to notify the Swiss National Cyber Security Center NCSC about the vulnerability.

Depending on the circumstances of the individual case, the NTC may adjust the level of detail of the publication.

6. Mutually agreed Early Disclosure

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

7. Credits

The NTC Vulnerability Disclosure Policy is inspired by the one proposed by Google's Project Zero. The Google Project Zero has many years of experience in disclosing vulnerabilities and provides valuable information and policies related to the topic.

- Google Project Zero Vulnerability Disclosure Policy
- Blog Post explaining Google Project Zero Policy and Disclosure: 2021 Edition
- Google Project Zero Vulnerability Disclosure FAQ