National Test Institute for Cybersecurity

NTC Vulnerability Disclosure Policy (VDP)

The NTC Vulnerability Disclosure Policy (VDP) applies to vulnerabilities discovered during security tests initiated by the NTC ("Initiative Projects"). The goal is to define processes and procedures for appropriate vulnerability disclosure that ensure both fairness to vendors and protection of civil society.

Version 2.0, 25. September 2024

1 Scope of application

1.1 The association «National Test Institute for Cybersecurity NTC» ("NTC") carries out cybersecurity tests of networked infrastructures, devices and applications. The NTC is operated on a public-private, not-for-profit basis.

1.2 Terminology:

a. Vendor for the purposes of this policy includes manufacturers, operators and distributors of products.
b. Manufacturer for the purpose of this policy shall mean the maintaining entity of the test object. In the context of Open Source Software (OSS), the term manufacturer entails the identifiable responsible maintainers of the OSS.

1.3 The Vulnerability Disclosure Policy (VDP) applies to NTC initiative projects concerning the testing of networked infrastructures, devices and applications, where no mandate or explicit consent of the vendor is provided.

1.4 Initiative projects are tests of networked infrastructures, devices and applications initiated and self-financed by the NTC to identify security vulnerabilities. The NTC decides independently what is tested and how intensively, based on experience, observations, information from partners and the public.

2 Communication and responsible disclosure

2.1 In compliance with the legal framework, vulnerabilities and the resulting risks are communicated as follows:

a. Vulnerabilities are communicated directly and initially exclusively to the manufacturer of the test object ("responsible disclosure").
b. Upon submission of the notification by the NTC, the manufacturer is granted 90 days from the time of reporting to fix the vulnerability. If possible, the notification will be addressed to the registered report address (e.g. security.txt). If affected third parties are required to take any action to protect themselves (e.g. to install a patch), the NTC may grant an additional 30 days upon availability of remediation measures.
c. For vulnerabilities that are fixed by the manufacturer within the granted period (section 2.1. lit. b.), the NTC will publish information on vulnerability patterns, for instance on https://hub.ntc.swiss. Public disclosure of fixed vulnerabilities is made with an extended level of details (e.g., vendor name, product title and vulnerability information) upon explicit or conclusive agreement from the manufacturer. In the absence of such an agreement, the NTC will publish vulnerability information with a reduced level of detail (e.g., without vendor name, product title or vulnerability information).
d. Vulnerabilities for which the manufacturer is unable or unwilling to provide a remediation within the granted period (section 2.1. lit. b.) may be disclosed with an appropriate level of details (e.g., vendor name, product title, and vulnerability information) for instance on https://hub.ntc.swiss.
e. Vulnerabilities that, in the judgment of the NTC, are considered to be of particular severity may also be reported directly to the Swiss National Cybersecurity Centre "NCSC" and the Swiss Federal Data Protection and Information Commissioner "FDPIC".