Responsible Disclosure Policy

CERT NRW

Basic information about CERT North Rhine Westphalia (NRW), its channels of communication and its roles and responsibilities according to RFC 2350 can be found on our website:
https://www.it.nrw.de/informationstechnik/Services/CERT/index.html

In order to help prevent harm and damage, CERT NRW shares threat intelligence and vulnerability information with its peers and partners in the information security community such as Deutscher CERT-Verbund (CV) and Verwaltungs-CERT-Verbund (VCV).

Basic Principles

CERT NRW sticks to the following principles for responsible disclosure of vulnerability information:

1. **Prevention of harm and damage**
   Our top priority is to alert and inform potentially affected users/organizations and enabling them to prevent harm and damage.

2. **Fairness**
   We also consider concerns and interests of the makers of affected products as long as in balance with our first basic principle. Circumstances of each individual case determine how, when and to which recipient group information is being disclosed.

3. **Transparency**
   By publishing these basic principles and the process described in the following sections, CERT NRW is transparent about how vulnerability information is being handled. CERT NRW wishes for a positive collaboration and coordinated disclosure with affected product makers and will always clearly communicate its proceedings in advance.

The second and third principles presume that affected product makers take security seriously, are willing to collaborate in a positive way, respond in a timely and non-bureaucratic manner, conduct a constructive dialogue and communicate clearly which steps they will take - and when - to mitigate and fix reported vulnerabilities.

Assessment, Categorisation and Handling of Vulnerability Information

According to the above second basic principle, circumstances determine how and when and to which recipient group information is being disclosed.

"Circumstances" means how easily and through which vectors a vulnerability can be exploited, as well as the potential impact this could have on affected target systems or data. Other things to take into account are population size (i.e. how widespread is the product in use), type of system (i.e. convenience service vs. critical infrastructure), availability of exploit code and if attacks in the wild already have been observed.

CVSS Scores

CERT NRW characterizes and prioritizes vulnerabilities using the Common Vulnerability Scoring System (CVSS[1]), which takes into account the above determining factors.

Scheme and Grades of Confidentiality Classification

Sharing of vulnerability information with partners and peers of CERT NRW are based on the Traffic Light Protocol (TLP[2]).

CERT NRW applies the following criteria for TLP classification:

- TLP-RED for highly critical vulnerabilities for which there is currently no mitigation, patch or protection available, which affect critical infrastructure, which are easily exploitable and therefore **premature public disclosure could cause large scale damage**.
- TLP-AMBER for all other vulnerabilities with no available patch, workaround or mitigation at that point in time.
- TLP-GREEN or TLP-WHITE for all other cases.

Other governmental classification schemes and legally binding regulations are not affected by this disclosure policy and are not described here (affects only information that has already been classified by other government bodies/organisations before reception by CERT NRW).

[1] https://nvd.nist.gov/vuln-metrics/cvss
[2] https://www.us-cert.gov/tlp

Confidentiality Classification Lifetime

TLP-AMBER information is downgraded to TLP-WHITE after a patch/fix becomes available.

45 days after first contact to the vendor TLP-AMBER information is downgraded to TLP-GREEN, regardless if a patch/fix is provided until then or not[3].

All TLP classified vulnerability information is downgraded to TLP-WHITE without further notification to vendors or manufacturers 1 year after first contact to the vendor, unless there are compulsive reasons to uphold the former classification. Requests for upholding the former classification need to requested by vendors / manufacturers in written form providing comprehensive reasons.

CERT NRW then decides and informs the vendor / producer of its decision after thorough consideration of all risks and benefits.

Dissemination and Publication

CERT NRW shares security information with other partner CERTs from industry and the public sector under TLP agreement.

Immediate dissemination to of vulnerability information to partner CERTs takes place if

- the vulnerability has a CVSS Base Score >=7
- the vulnerability already is or has been actively exploited

In those cases dissemination usually takes place on a need-to-know basis (TLP-AMBER) or TLP-RED, as long as the information has not already been classified using another binding governmental classification scheme, before reception by CERT NRW.

In all other cases, vulnerability information is shared with partner CERTs 30 days after notifying the vendor/producer of the product.

TLP-WHITE information is disclosed to the general public if CERT NRW regards it necessary to comply with its first basic principle (prevent harm) and if the information enables users to protect themselves.

CERT NRW will never publish exploit code but only warnings and preventative guidance.

[3] As a comparison: CERT/CC even publishes all vulnerabilites after 45 days regardless if a fix is available or not: https://www.cert.org/vulnerability-analysis/vul-disclosure.cfm

Approaching Product Makers

Whenever CERT NRW becomes aware of any previously unknown vulnerability, we will seek to contact the vendor / producer in order to inform them as soon as possible.

CERT NRW will first try to contact the official CERT or PSIRT (product security incident response team) of the vendor or affected producer. Therefore we advise vendors / producers to make this contact information easily accessible through their company website.

We will also inform the vendor / producer about the TLP classification and planned dissemination to our partners.

We also share all information we have about the vulnerability with the producer and will reply to any follow-up questions about technical details and our assessment.

We will do our best to consider the producer's interests and concerns as long as they don't clash with our basic principles of prevention, fairness and transparency.

A scheduled publication or declassification / downgrade can be postponed for up to three months if – and only if – we are convinced of the vendor's / producer's full cooperation, their plausible justification and if, after careful consideration, we think it is justifiable under our 1st principle.

We will not postpone in one or more of the following circumstances:

- attacks or exploits against the vulnerability have already been observed in the wild,
- the vulnerability is trivially exploitable (e.g. simply typing a specific url),
- the vulnerability is very exposed, widespread and easy to find for attackers.