One Year of Responsible Disclosure

Ivo Dijkhuis
Overview

1. Why a Responsible Disclosure Policy
2. Our Responsible Disclosure Policy
3. Some statistics
4. Lessons learned
Why a Responsible Disclosure Policy?

1. We support the idea of Responsible Disclosure

2. We want to be transparent to our community

3. Make it easier to report a (suspected) security vulnerability

4. The need for better incident coordination internally

5. Single point of contact - RIPE NCC CSIRT
Our Responsible Disclosure Policy (1)

• Single point of contact: security@ripe.net

• Easy to find: http://www.ripe.net/security

• Reporter can remain anonymous and we offer the option to use (PGP) encryption.

• We strive to respond within three business days with our evaluation of the issue and resolution date; all reports will be handled with strict confidentiality.
Our Responsible Disclosure Policy (2)

• We ask to provide sufficient information so we can reproduce the problem.

• We request the reporter does not take advantage of the issue and does not publish any details before we were able to fix the issue.

• We do not threaten with legal actions.

• If desired, we will credit the findings to the reporter, when we publish a report on the security issue.
Some statistics

• Pre-Responsible Disclosure Policy reports: ?

• Since the introduction of the policy: 62 reports

  • Spam: 7 (11%)
  • Non-security issues: 27 (44%)
  • Minor issues: 24 (39%)
  • Major issues: 4 (6%)
Lessons learned

- Need a ‘hall of fame’, also for minor issues

- No bug bounty programme - but need a reward

- Response templates - especially for non-security issues

- A resolution date is hard to set

- Involve senior management & your communications department early