Coordinated Vulnerability Disclosure Manifesto

Over the last decades, the importance of ICT and the role it plays in our everyday lives has increased exponentially. As our interconnectedness grows and the dependence of our societies on the Internet and ICT increases, the potential negative impact of vulnerabilities in ICT also increases. Consequently, finding and remedying those vulnerabilities is increasingly important.

Cooperation between organizations and the cyber security community can be helpful in finding and fixing vulnerabilities. A mechanism of cooperation that is already used in that regard is *coordinated vulnerability disclosure* or *responsible disclosure*. Essentially, this is a form of cooperation in which vulnerabilities are reported to the owner of the information system, allowing the organization the opportunity to diagnose and remedy the vulnerability before detailed vulnerability information is disclosed to third parties or the public. Further publication will be coordinated between the finder and the organization.

With this manifesto, initiated by Rabobank and CIO-Platform Nederland, the signing parties try to raise awareness for the importance of cooperation between organizations and the ICT-community to find and solve ICT-vulnerabilities. In the experience of the initiators, such cooperation results in many vulnerabilities being reported and consequently mitigated or remedied. This shows that cooperation actually works and can be extremely helpful in improving the security of information systems on which our economies and societies are so dependent. This Manifesto underlines this conclusion and is meant to show that organizations are committed to reaping the benefits of such cooperation with the cyber security community.

The signatories of this Manifesto are committed to:

- acknowledge the efforts of (academic) researchers, penetration testers, passersby, observant users and customers, employees, well-intended hackers and everyone else to make the internet and our society more secure;
- combine the efforts of their organization and the cyber security community in realizing a safe and secure digital society;
- strive to remediate vulnerabilities in a correct and timely fashion;
- combine efforts to follow international standards and best practices for remediating and disclosing vulnerabilities and implementing these in their organization. A non-comprehensive list with information on such standards and best practices can be found in Appendix A;
- be transparent in providing information about the remediation and disclosure process;
- join efforts to stimulate the development of international standards and best practices for remediating and disclosing vulnerabilities;
- stimulate the international dialogue to promote the use of those mentioned mechanisms of cooperation for remedying and disclosing vulnerabilities; and
- actively advocate the contents of this manifest to peers.

Taking in account that the finder of the vulnerability:

- will agree on terms and conditions for disclosure of vulnerabilities found;
- acts in good faith; and
- will not act disproportionately (i.e. cause unnecessary damage) when trying to find and disclose vulnerabilities.

By signing this Manifesto I express my intention of implementing Coordinated Vulnerability Disclosure in my organization.

Name		
Jobtitle		
Organization		
Place	**Date**	
Signature		

Appendix A

- ISO/IEC 29147:2014[1]
  - This standard helps guide organizations on how to receive vulnerability reports from parties outside your organization, and how to disseminate vulnerability advisories
- ISO/IEC 30111:2013[2]
  - This standard describes guidelines on how to process and resolve potential vulnerability information in a product or online service
- CIO Platform Nederland: Coordinated Vulnerability Disclosure Implementation Guide[3]
  - This guide helps organizations with implementing their own coordinated vulnerability disclosure policy in their organization
- CIO Platform Nederland: Coordinated Vulnerability Disclosure Model Policy and Procedures[4]
  - Provides a model policy and procedure for organizations for handling and remediating vulnerabilities
- NCSC Responsible Disclosure Guideline[5]
  - The guideline or policy for arriving at a practice for Responsible Disclosure is a tool for organizations and incident reporters to facilitate reporting and handling of vulnerabilities in information systems, software and other ICT products. Organizations can use the guideline to help them draft their own policies
- GCCS Best practice guide Responsible Disclosure[6]
  - This document describes the policy side of implementing responsible disclosure and practical experiences by public and private parties
- ENISA Good Practice Guide on Vulnerability Disclosure[7]
  - This study seeks to achieve to take stock of the current situation in vulnerability disclosure; identify the challenges of the current situation with respect to vulnerability disclosure; identify good practices; and propose recommendations for improvements to address the challenges and enhance the adoption of good practices

[1] http://www.iso.org/iso/catalogue_detail.htm?csnumber=45170
[2] http://www.iso.org/iso/catalogue_detail.htm?csnumber=53231
[3] http://www.cio-platform.nl/uploads/CioPublicatie2016%20CegInfoSec%20Coordinated%20Vulnerability%20Disclosure%20Implementation%20Guide%20-%20ENG%20v1.0.pdf
[4] http://www.cio-platform.nl/uploads/CioPublicatie2016%20CegInfoSec%20Coordinated%20Vulnerability%20Disclosure%20Policy%20and%20Procedure%20-%20ENG%20v1.0.pdf
[5] https://www.ncsc.nl/english/current-topics/news/responsible-disclosure-guideline.html
[6] https://www.gccs2015.com/sites/default/files/documents/BestPracticeRD-20150409_0.pdf
[7] https://www.enisa.europa.eu/activities/cert/support/vulnerability-disclosure