Coordinated Vulnerability Disclosure

Jeroen van der Ham
“Everybody has vulnerabilities, being able to receive them and respond to them is what matters”
Vulnerability Disclosure

- *Coordinated* vulnerability disclosure (CVD)
  - Working with vendors to fix vulnerabilities before disclosure
  - Phases: Report, Triage, Develop, Deploy
  - CVD happens *before* vulnerability management
- Disagreement, debate, and some agreement for 30+ years
  - Responsible? Coordinated?
  - What information, to whom, when
  - How long to wait for vendor
Governments

- Didn’t pay that much attention until...
  - Everything became a connected computer
    - Including safety-regulated sectors like transportation, health care, manufacturing
  - Introduction of liability for software systems
  - National and international efforts

Source: Wired

Source: Motortrend

Source: LIXIL
and You

• A defender
• Directly or indirectly use systems that are connected and vulnerable
• Don’t know what all the components are nor where they exist (nor do your vendors and providers)
• Not a cyber-security expert
  ›Rough analogy: Operating a car without understanding completely how it works
• Disclosure provides information to you and your vendors and providers to assess and mitigate risk
Many international CVD initiatives & guidelines

**Initiatives**

- GFCE
- NTIA
- DEPARTMENT OF JUSTICE

**Publications**

- GCCS 2015
- NCSA
- ISO

ISO 29147 & 30111
Situation in The Netherlands
Coordinated Vulnerability Disclosure Manifesto

Download the manifesto at www.thegfce.com
Bug Bounties
THE WASSENAAR ARRANGEMENT

ON

EXPORT CONTROLS FOR CONVENTIONAL ARMS

AND

DUAL-USE GOODS AND TECHNOLOGIES
5. A. 2. a. 1. a. A "symmetric algorithm" employing a key length in excess of 56 bits; or

*Technical Note*
In Category 5 – Part 2, *parity bits are not included in the key length.*

b. An "asymmetric algorithm" where the security of the algorithm is based on any of the following:
1. Factorisation of integers in excess of 512 bits (e.g., RSA);
2. Computation of discrete logarithms in a multiplicative group of a finite field of size greater than 512 bits (e.g., Diffie-Hellman over $\mathbb{Z}/p\mathbb{Z}$); or
3. Discrete logarithms in a group other than mentioned in 5.A.2.a.1.b.2. in excess of 112 bits (e.g., Diffie-Hellman over an elliptic curve);
4. A. 5. Systems, equipment, and components therefor, specially designed or modified for the generation, operation or delivery of, or communication with, "intrusion software".

4. E. 1. "Technology" as follows:

c. "Technology" for the "development" of "intrusion software".
"Intrusion software"

"Software" specially designed or modified to avoid detection by 'monitoring tools', or to defeat 'protective countermeasures', of a computer or network-capable device, and performing any of the following:

a. The extraction of data or information, from a computer or network-capable device, or the modification of system or user data; or

b. The modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions.

Notes
1. "Intrusion software" does not include any of the following:
   a. Hypervisors, debuggers or Software Reverse Engineering (SRE) tools;
   b. Digital Rights Management (DRM) "software"; or
   c. "Software" designed to be installed by manufacturers, administrators or users, for the purposes of asset tracking or recovery.

2. Network-capable devices include mobile devices and smart meters.
Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

setting up a Union regime for the control of exports, transfer, brokering, technical assistance and transit of dual-use items (recast)

{SWD(2016) 314 final}
{SWD(2016) 315 final}
Timeline

• 2013: Discussion in Wassenaar Arrangement
• dec 2013: introduction of “Intrusion Software”
• 31 dec 2014: Update of EU Regulation:  
• jul 2015: consultation in US
• aug 2015: thousands of responses in US
Coordinated Vulnerability Disclosure building blocks

Promises of the organization (CVD policy)

Responsibilities of the researcher or ethical hacker

www.ncsc.nl
Example pages
Example rewards

Or: bug bounties (€)
CVD building blocks (responsibilities of researcher / ethical hacker)

- Timely disclosure
- Confidentiality
- Proportionate
- Least invasive method

- No brute forcing
- No backdoors
- No malware
- No alteration of data
- No social engineering
NCSC statistics of # of CVD reports
Case: Groene Hart Hospital

Source: www.ghz.nl

Case details

• Dutch public hospital with vulnerable FTP server with easily brute forceable administrator credentials (password: groen2000)
• Hacker finds the vulnerability and informs a journalist
• Journalist informs the hospital at 10:00 and publishes the story at 15:00
• The hospital reports the case to the police
• The hacker used a port scan tool (Nessus) for two weeks (using VPN)
• The hacker probably retrieved the password hashes used by the FTP-server and bruteforced them
• The hacker shares the credentials with other persons
• The hacker installed malware on the server, using his own IP
• The hacker downloaded multiple medical files, including those of famous people
• The hacker sent screenshots of those files to a journalist
• The hacker states that its actions were in the public interest
Groene Hart Hospital

Outcomes:

• Public Prosecutor Service has discretion to prosecute. Judge will have to judge whether the actions of the ethical hacker were proportionate and subsidiary.
• Judge emphasizes that revealing security vulnerabilities can be in the public interest, especially when sensitive (medical) files are at stake.
• The judge finds that there were no other ways for the hacker to discover the vulnerability (least invasive)
• The judge finds that installing the malware was necessary to show that the network of the hospital had weak security.
• However, the hacker accessed the server and downloaded data multiple times, including data about famous people. This was not necessary to proof the vulnerability.

• **Sentence: 120 hours of community service**
Diagnostiek voor u (ECLI:NL:RBDHA:2014:15611)

Case details

• Discloser is politician and journalist (HK)
• Acquaintance of discloser discovers login/pass of a medical system
• Discloser does reconnaissance, prints a few files and anonymises them.
• Discloser calls helpdesk and asks for written report.
• Discloser calls local TV station, tells them about findings.
• Demonstrates to journalists logging in, and shows some patient files, on camera.
Diagnostiek voor u

**Verdict**

- Judge stresses that disclosing vulnerabilities of sensitive (medical) systems can be in general interest.
- It was reasonable to test the initial findings in practice.
- It is defensible that the discloser prints a few medical files and anonymises them, to prove the vulnerability.
- The judges uses a three part test in light of article 10 ECHR (freedom of expression and information)
  1. Discloser should act in general interest
  2. Discloser should act proportionately
  3. Discloser should act in least invasive way
Diagnostiek voor u

Verdict

• Proportionality:
  • It was not necessary to review the files with a journalist

• Invasiveness:
  • There was no reason to go to the media. There was no big vulnerability that everyone could exploit. There were no indication that anyone else had the credentials.
  • The suspect should have taken more effort to contact the responsible party. As member of parliament and journalist it reasonable to expect him to take more effort for contact.

• Result: €1500 fine
Case: KPN
Case details:

- Two ethical hackers find vulnerabilities in modems.
- The modems are widely used by KPN and its customers.
- The vulnerabilities give complete remote access to modems.
- The vulnerability can be misused for DDoS attacks and to intercept data.
- Hackers tested the vulnerabilities against their own modems.
- The ethical hackers reported the vulnerabilities to KPN.
KPN

Case outcome:
• CERT of KPN takes up the report
• KPN invites the ethical hackers to its office to show and explain their findings
• The vulnerabilities get fixed within a short amount of time
• The ethical hackers are rewarded with KPN ‘goodies’ and are allowed to present their findings at a congress
• KPN uses the case to show that it takes the security of its customers and network very seriously
• KPN releases a press statement on its website and creates an informative video to promote its CVD policy and cooperation with ethical hackers
Researcher motivation

Source: NTIA report: Vulnerability Disclosure Attitudes and Actions
Key takeaways

• Governments take Vulnerability Disclosure seriously

• Coordinated Vulnerability Disclosure policy does not give hackers a carte blanche

• More and more organisations appreciate and cherish involvement of the security research community
Questions?

Comments?

- <jeroen.vanderham@ncsc.nl>
- B0EB 8533 A34B 0F9B 3FC7  3850 83E7 A228 CCA0 23F0
- Twitter: @1sand0s