



National Cyber Security Centre
Ministry of Security and Justice

Coordinated Vulnerability Disclosure

Jeroen van der Ham

NCS C



Some facts

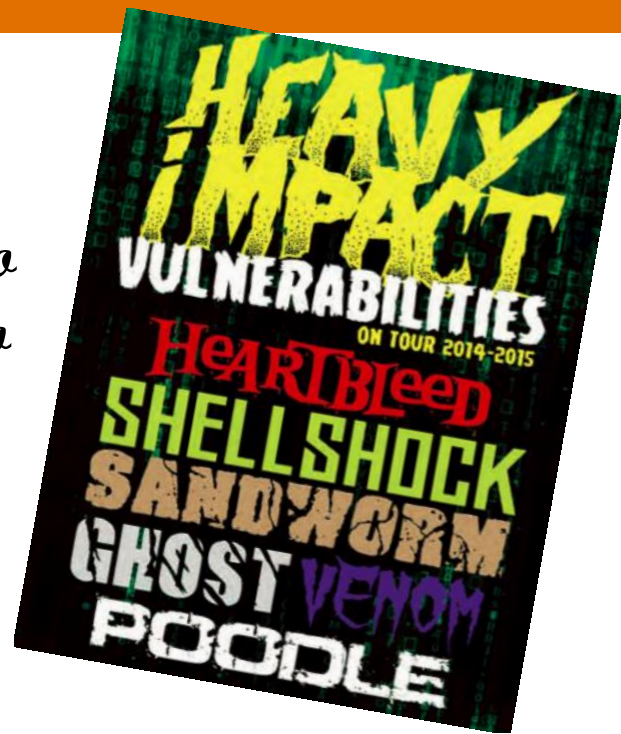


By Source (WP:NFCC#4), Fair use, Wikipedia.org



Drown

“Everybody has vulnerabilities, being able to receive them and respond to them is what matters”



Source: Cyber Security Assessment Netherlands 2015, image creator Ken Westin



Undesirable situations



159.46.193.36
is vulnerable!

Afraid to report
vulnerabilities



Panic
!



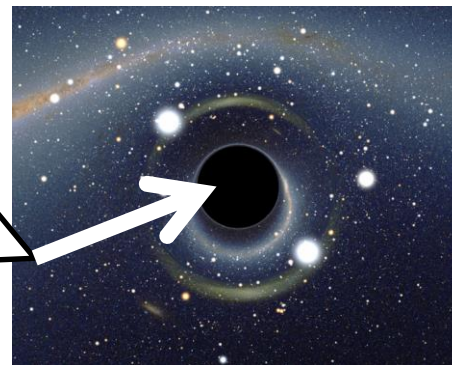
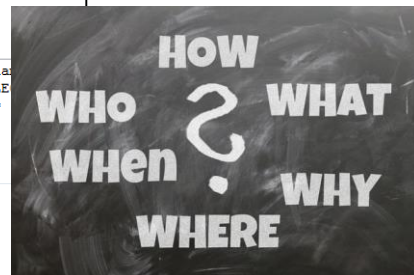
I found a
vulnerability in your
system! Gimme
money! Grz H4x0r!

User Name:

E-mail address:

```
SELECT * FROM users WHERE na  
= 'a'; DROP TABLE users; SELE  
* FROM userinfo WHERE 't' =
```

Comments:





Many international CVD initiatives & guidelines

Initiatives

- Global Forum on Cyber Expertise (GFCE) Cyber Security Coordinated Vulnerability Disclosure Initiative
- USA National Telecommunications & Information Administration (NTIA) Cybersecurity Vulnerabilities Multistakeholder Process



Guidelines

- ENISA Good Practice Guide on Vulnerability Disclosure
- GCCS Best practice guide Responsible Disclosure
- ISO/IEC 29147:2014 and ISO/IEC 30111:2013
- Responsible Disclosure policy guide (NL)





Coordinated Vulnerability Disclosure Manifesto

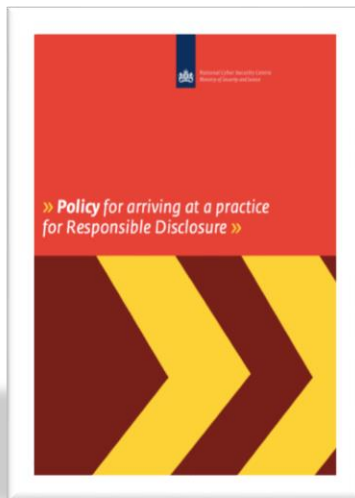


Palo Alto Networks, Vodafone, Phillips, Honeywell, Rabobank, CIO Platform Nederland, ABN AMRO, CIOforum Belgian Business, Corbion Group Netherlands, Eneco, European Network for Cyber Security, IHC Merwede, ING, KPN, LUMC, NS, NUON, NXP, PostNL, SAAB, Schuberg Phillis, SNS Bank, Stedin, Surfnets, Tennet, TNO and VOICE.



Coordinated Vulnerability Disclosure building blocks

Promises of
the
organization
(CVD policy)




www.ncsc.nl

Responsibilities
of the
researcher or
ethical hacker



Example pages



Particulieren Private Banking

Rabobank

< Veilig bankieren

Kwetsbaarheden melden


Heeft u een probleem of zwakke plek gevonden in onze scripting kwetsbaarheden, SQL-injectie kwetsbaarheden om het probleem niet publiek te maken maar te delen.

Als u een kwetsbaarheid meldt die door ons wordt verteld dienstverlening leidt, dan ontvangt u als dank een pass is niet bedoeld voor het melden van bijvoorbeeld valse internetbankieren.

U kunt kwetsbaarheden op twee manieren bij ons melden:

1. Melden via een versleutelde e-mail

Stuur ons een versleutelde e-mail waarin u het probleem kort en bondig beschrijft in het Nederlands of Engels. Gebruik voor het versturen van de e-mail de PGP-key die u hieronder kunt downloaden. Een team van beveiligingsexperts onderzoekt uw melding. Geef hen de tijd om het probleem op te lossen. U hoort zo snel mogelijk wat we van uw melding vinden, of we een oplossing gaan toepassen en wanneer we dat gaan doen.



LANDLIGERS

PRODUCTS & SERVICES PARTNERS

ABOUT US

From Internet-wide research to product innovation to thought leadership in network security and management for today's networks


Responsible Disclosure Policy

Arbor's Commitment

Arbor Networks' products are trusted to protect the world's largest, most distributed systems that trust and keep our customers safe, we investigate and respond to vulnerability reports. We place a high priority on responding to any security concerns related to our products.

In the best interest of our customers and Internet users worldwide, we ask that you follow these guidelines:

- Do not publicly disclose part or all of the vulnerability until we have had a chance to respond.
- Do allow us a reasonable timeframe to respond back to you and address the vulnerability.
- If you are customer, do patch your system as quickly as possible. It is customary to patch within 30 days after release of a security patch or update. We advise our customers that those who exploit security systems often do so by reverse engineering published security updates and therefore encourage our customers to patch promptly.



National Cyber Security Centre
Ministry of Security and Justice

Home Current topics Incident Response Expertise & Advice Cooperation Organisation Conference Sitemap Advanced search

Home > Incident Response > Responsible Disclosure Report

Responsible Disclosure Report


The National Cyber Security Centre (NCSC) contributes to jointly enhancing the resilience of the Dutch society in the digital domain and, in doing so, realises a safe, open and stable information society by providing insight and offering a perspective for action. Therefore it is essential that the ICT systems of the NCSC are safe. The NCSC strives towards providing a high level of security for its systems. However, it can occur that one of these systems has a vulnerability.

Vulnerabilities in ICT systems of the NCSC

If you have found a weak spot in one of the ICT systems of the NCSC, the NCSC would like to hear about this from you, so the necessary measures can be taken as quickly as possible to rectify the vulnerability. To deal with the vulnerabilities in the NCSC ICT systems responsibly, we propose several agreements. You may hold the NCSC to this when you discover a weak spot in one of our systems.

The NCSC asks you:

- 1. To e-mail your findings to cert@ncsc.nl. Encrypt your findings if possible with the PGP key of the NCSC to prevent the information falling into the wrong hands.
- 2. Provide sufficient information to reproduce the problem so that the NCSC can solve the problem as quickly as possible. The IP address or the URL of the system affected and a description of the vulnerability is usually sufficient, but more may be needed for more complex vulnerabilities.
- 3. Leave your contact details so that the NCSC can contact you to cooperate on a safe result. At least, leave an e-mail address or a telephone number.
- 4. Report the vulnerability as quickly as possible after its discovery.





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





Case: Groene Hart Hospital



Source: www.ghz.nl



Groene Hart (ECLI:NL:RBDHA:2014:15611)

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**



Case: KPN





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



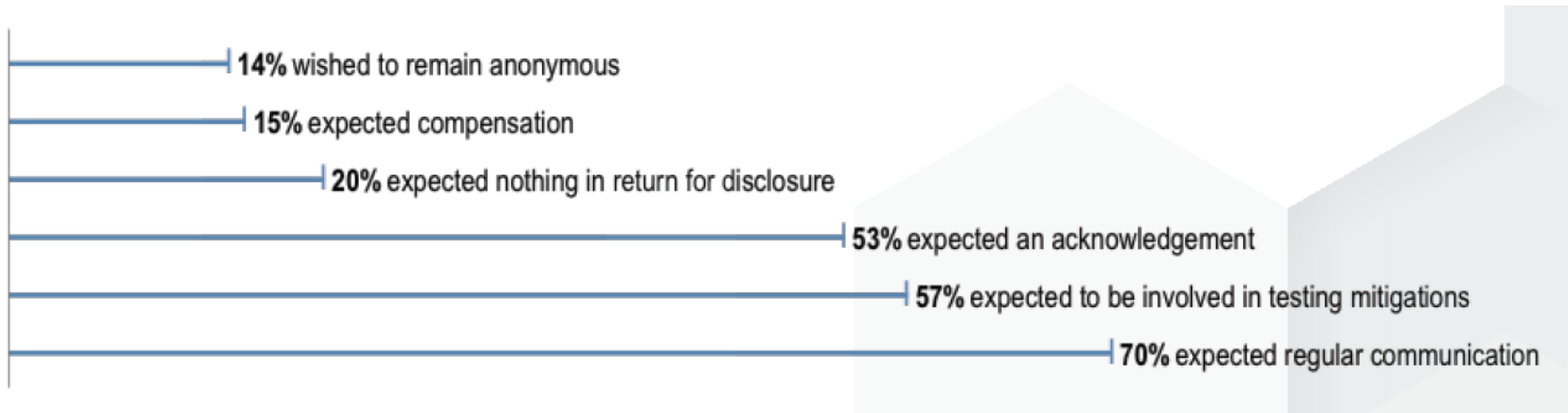
KPN

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

<https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities>



Key takeaways

- Secure software does not exist, receiving and responding to vulnerabilities is what matters
- Coordinated Vulnerability Disclosure policy does not give hackers a carte blanche
- Appreciate and cherish involvement of the ethical hackers and security research community