National Cyber Security Centre
Ministry of Justice and Security

Coordinated Vulnerability Disclosure: The Guideline

Preface

Until the beginning of this decade, reports about digital vulnerabilities were not received with open arms. Holes in ICT-systems would simply go unclosed. Cybercriminals happily used these to attack public and private organizations. How different is this practice in 2018!

The National Cyber Security Centre (NCSC) stimulates the process of Coordinated Vulnerability Disclosure (CVD) actively since the publication in 2013 of the 'guideline to come to a practice of responsible disclosure'. The hundreds of reports that the NCSC has received since then illustrate the trust and cooperation that exists in the ICT community, governments, companies and the NCSC for a CVD process that aims to resolve vulnerabilities in hard- and software.

I am proud that I may introduce the reviewed product of this fruitful cooperation. A product that puts the human first, as that is what CVD is about. 'Coordinated Vulnerability Disclosure – the guideline' is an improvement of the process with the most important lessons from the 5 years of practical experience. A result that will be internationally shared and propagated.

With the presentation of this guideline, we take another step towards a digitally secure Netherlands.

Hans de Vries
Director NCSC

Rickey Gevers

1. Introduction

Society is increasingly digitalising. These days, almost all processes involve the use of computers at some point, ranging from mobile phones to specialised software. Although this development creates many new opportunities, vulnerabilities in IT systems can have a major impact. As a result, knowledge about these vulnerabilities should be dealt with effectively.

A number of organisations started publishing policy on how to report vulnerabilities at the beginning of 2013. After consultation with these parties, the National Cyber Security Centre (NCSC) summarised the developments in the form of 'Guidelines for achieving a Responsible Disclosure practice' ('Leidraad om te komen tot een praktijk van Responsible Disclosure'; the 'Guidelines'). Companies indicate through this policy that they are open to receiving external vulnerability reports, describe their preconditions and make promises. This process created clarity and a somewhat safe environment for reporting parties to investigate and report vulnerabilities without directly committing a criminal offence. At the EU high-level meeting on cyber security in 2016, 29 organisations reaffirmed the importance of a policy for dealing with vulnerabilities by signing the Coordinated Vulnerability Disclosure Manifesto[1] initiated by the CIO Platform Netherlands and Rabobank in cooperation with the NCSC.

Coordinated Vulnerability Disclosure (CVD) has proved to be of great importance for public and private parties. They are highly dependent on the undisturbed functioning of information systems in daily practice. Reports of vulnerabilities in their systems have helped to improve the security and continuity of systems in recent years, by remedying vulnerabilities on the one hand and by contributing to Dutch companies' general awareness of IT security on the other.

In recent years, it has become clear that reporting parties are prepared to work within the conditions of the CVD policy drawn up by organisations. Reports are made directly or indirectly to organisations by reporting parties. Responsible disclosure practice has shown that well-intentioned reporting parties and vulnerable organisations have managed to cooperate and thus take the next step in increasing the security of network and information systems.

For this revision, we once again talked with a broad and diverse group of reporting parties, private and public parties, as well as the Public Prosecution Service and the National Police. These conversations have confirmed the current practice, and led to additions and improvements. The most important new point of attention is communication between vulnerability reporter and organisation, as well as with other parties after a vulnerability has been remedied.

The following chapters discuss the definition of CVD, the building blocks for a CVD policy and the communication process.

The previous Guidelines used the term 'responsible disclosure', which was the common term for this practice at the time. It has meanwhile become clear that this term places too much emphasis on the responsibility of the reporting party, while the basic principle is that the reporting party and the potentially vulnerable organisation should be equal partners in the dialogue. This sentiment is better captured in the current commonly used term 'Coordinated Vulnerability Disclosure' (CVD), which is also the name used in the ISO 29147 and 30111 standards on this process.

1 https://www.thegfce.com/initiatives/r/responsible-disclosure-initiative-ethical-hacking/manifesto

Melanie Rieback

2. Coordinated Vulnerability Disclosure

Various methods have been used over the past 30 years to raise awareness of vulnerabilities in IT systems. Examples include:

- **'Full Disclosure', making a vulnerability fully public;**
- **'Non-disclosure', selling or using a vulnerability yourself;**
- **'Coordinated Vulnerability Disclosure' (CVD), the coordinated disclosure of a vulnerability.**

The latter practice is expressly preferred.

The IT-community has shown great willingness to share knowledge and experience. Seeking cooperation with this community can therefore help to improve the overall security of systems.

The Aim of Coordinated Vulnerability Disclosure

The aim of CVD is to contribute to the security of IT systems by sharing knowledge about vulnerabilities. In CVD, knowledge is shared with one or more potentially vulnerable organisations in order to arrive at a joint solution for the vulnerability found in collaboration with the reporting party. It is important that the organisations affected have sufficient time to remedy any vulnerabilities or protect systems in order to limit or prevent loss or damage as much as possible. The cornerstone of the process is disclosure of knowledge about the vulnerabilities after remediation.

It is essential in CVD that all parties comply with agreements on how to report a vulnerability and how to deal with it. What helps is if an organisation publishes preconditions in advance, such as which systems are within scope and what kind of research can be conducted. An important principle for these preconditions is that the organisation will not report the reporting party in principle or take other legal steps if the investigation and reporting is carried out within the conditions set. These Guidelines provide organisations with guidance in drawing up their own policy to embody the principles of CVD.

As the name indicates, it is central to CVD that the organisation and the reporting party coordinate with each other. In this respect, there should be as few links as possible between the person reporting the vulnerability and the person within the organisation who is responsible for solving the problem.

It may be important to inform several parties at the same time if a vulnerability affects many systems. In that case, the NCSC or other parties within the security community can support the CVD process from a coordinating role.

Mischa R. van Geelen

3. Areas of responsibility

The aim of pursuing a CVD policy is for the reporting parties and the organisation to work together in order to reduce the vulnerabilities in IT systems. Implementing this policy should be seen as a supplement to existing measures on information security. The various actors each have their own role and responsibilities. These are explained in more detail below.

The organisation that owns/manages a system

The organisation that owns/manages or supplies a system is primarily responsible for the security of this system. In other words, the organisation is also responsible for following up on a vulnerability report.

The organisation may choose to draw up its own CVD policy using these Guidelines and to communicate this policy with potential reporting parties. By publishing a CVD policy, organisations show their willingness to receive information about vulnerabilities. A party establishing a CVD policy can commit to the principle that it will not file a complaint with the police if the rules that apply to the policy are respected.

Once a reporting party has reported a vulnerability, the responsibility lies with the organisation. It is important to realise that the reporting party is often someone outside the organisation. This party does not have a direct view of the internal processes that can be triggered after a vulnerability has been reported. As a result, reporting parties will appreciate being informed of developments in the resolution of the vulnerability. This ongoing communication is also important in order to create the right expectations for the follow-up and timeliness of the solution.

The party reporting a vulnerability

In one way or another, the reporting party has been able to identify a vulnerability and wants to contribute to the security of IT systems by having this vulnerability remedied and possibly made public at a later stage. The reporting party may have discovered something through passive observation or by actively testing the IT system. Of course, this party is responsible for their own actions and the way in which they discovered the vulnerability. It is the reporting party's own responsibility to be aware of the conditions set by an organisation in its CVD policy. Most governments and companies have published their CVD policies on their websites.

Finding vulnerabilities may nevertheless involve breaking the law. In the context of the CVD, the organisation and the reporting party can agree that any criminal acts they will not file a report. With this regard, the CVD policy published by the organisation is the guiding principle. The parties can also agree that no civil action will be taken.

If there is a suspicion that the law has been broken by the reporting party, a CVD policy can first of all help to prevent the reporter from being reported to the authorities. This procedure depends entirely on the preconditions of the policy with which an organisation requires a reporting party to comply and whether this compliance has been achieved, potentially with a corresponding promise not to file a criminal complaint as long as the party operates within the conditions of the policy. If a police report is made, the existence of and compliance with a CVD policy is a relevant circumstance in the Netherlands, which the Public Prosecutor will take into account when deciding whether to initiate a criminal investigation and/or to prosecute. In principle, the police and the Public Prosecution Service (OM) will not initiate a criminal investigation if the reporting party has clearly complied with the rules of the CVD policy from the organisation in question. However, the Public Prosecution Service and the police can investigate the case further if there are indications that the reporting party has consciously or unconsciously gone too far in their actions and/or failed to comply with the CVD policy. Based on this investigation, the Public Prosecution Service can decide whether to prosecute.

The Public Prosecution Service has published a policy letter in which it deals more specifically with aspects that are important in arriving at a decision to investigate and/or prosecute. For example, whether the reporting party's actions served an important public interest, whether the party acted disproportionately and whether the party could perhaps have acted in another, less drastic manner. The relevant policy letter further elaborates on these aspects.[2] Relevant case law since 2013[3] shows that these aspects are also taken into account in court if an organisation does not have a CVD policy.

2 https://www.om.nl/@32028/beleid-ethische/

3 See http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBOBR:2013:BZ1157 and http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBDHA:2014:15611

Victor Gevers

4. Building blocks of the Coordinated Vulnerability Disclosure process

Building blocks in shaping the CVD process for the organisation, the reporter and the NCSC are provided below.

4.1 The organisation

Promoting CVD starts with an organisation that owns IT systems or that supplies an IT product/system. After all, this organisation is primarily responsible for the information security of these IT systems. In order to work effectively with various parties to resolve vulnerabilities, an organisation may decide to draw up and publish a CVD policy. Drawing up its own CVD policy allows the organisation to demonstrate how it deals with reports of vulnerabilities. This way, an organisation can also give shape to the way in which it wishes to receive notifications. Such a process can be organised as follows:

- The organisation establishes and publishes a CVD policy.
- In this policy, the organisation provides clear rules for the research that reporting parties can carry out, such as which techniques are permitted and which systems are within or out of scope.
- The organisation makes it easy for a reporting party to make a report. One option is the use of a standardised reporting method; for example, a specific email address or online form. In addition, the organisation can decide whether to accept anonymous reports.
- The organisation reserves internal capacity and sets up a process in order to respond adequately to reports. It is advisable to set up a process with which any vulnerabilities found can be adequately remedied. In this respect, the origin of the report is irrelevant. The vulnerability may also have been identified by an internal employee or during a test, for example.
- Practical experience shows that there will be a greater interest in reporting vulnerabilities to the organisation after the initial publication of a CVD policy. The organisation should consider this when planning (extra) capacity.
- When the organisation receives the vulnerability report, it ensures that the report reaches the department that is best suited to assess and deal with the report as soon as possible.
- The organisation sends an acknowledgement of receipt of the report to the reporting party, preferably signed digitally to emphasise the priority.
- Subsequently, the organisation will enter into consultation with the reporting party in order to determine the period within which any publication will take place. This period will depend heavily on the nature of the vulnerability and the type of system.
  - As a guideline, a period of approximately 60 days is often used for software vulnerabilities. Remedying vulnerabilities in hardware is more difficult to achieve; a guideline of 6 months can be used.
- It may be desirable to extend or shorten this period by mutual agreement depending on how many or few IT systems depend on the system for which the vulnerability was reported or if the vulnerability is easier or more difficult to resolve.
- A vulnerability may prove difficult or impossible to resolve, or there might be high costs involved in resolving it. In such cases, the organisation may agree to regard the vulnerability as an accepted risk and not to remedy it, possibly in consultation with the reporting party.
- The organisation will keep the reporting party informed about the development of the process.
- In addition, the organisation can offer that the reporting party is publicly acknowledged for publishing the vulnerability. It is also possible to opt for a joint disclosure to the outside world.
- It is preferable to reward the reporting party for reporting vulnerabilities in systems if the party has complied with the

rules of the CVD policy. The amount of the reward may depend on the quality of the report. Rewarding the reporting party can create a better relationship between that party and the organisation, as well as increase people's willingness to make new reports in accordance with the CVD policy.
- In consultation with the reporting party, the organisation can agree to inform the wider IT community about the vulnerability if it is plausible that the vulnerability is also present in other places.
- In its CVD policy, the organisation can commit itself to the principle that it will not file a complaint with the police if the reporting party has complied with the rules as outlined in the policy.

4.2 The reporting party

The reporting party is the key to a successful CVD process. In one way or another, this party has been able to identify a vulnerability, and wants to contribute to the security of IT systems by having this vulnerability remedied by an organisation and made public. In doing so, reporting parties acknowledge that they can make an important contribution to society by revealing vulnerabilities in a coordinated manner. In order to achieve a successful CVD process, the following building blocks are important to the reporting party:

- The reporting party is responsible for its own actions and must observe the principles of proportionality as well as subsidiarity when investigating and reporting vulnerabilities. In other words, the reporting party should not do more than what is necessary to demonstrate the vulnerability and should always report the vulnerability to the system/information owner first.
- The reporting party must report the problem as soon as possible in order to prevent malicious parties from discovering the vulnerability and taking advantage of it.
- The reporting party must make the report to the organisation in a confidential manner to prevent others from gaining access to this information.
- The reporting party may not make the filing of a report or the further provision of information dependent on the reward. The initiative for granting a reward in the event of a report lies with the receiving organisation, which can outline preconditions in its published policy.
- The reporting party and the organisation make clear agreements on the disclosure of the vulnerability. If more than one organisation is involved, the basic principle is that the vulnerabilities can only be published if all organisations agree to this fact. Making these agreements at an early stage is advisable.
- The reporting party and the organisation involved can make agreements on informing the wider IT community. For example, this situation may apply to a vulnerability (whether or not already known) that is known to be present in more than one location. The National Cyber Security Centre (NCSC) can be involved in this process to support the target groups of the central government and critical infrastructure or to inform several parties in the event of a vulnerability that affects many systems.

4.3 The NCSC

The CVD process is primarily a matter for organisations and reporting parties. Nevertheless, the NCSC will encourage the use of a CVD process. In consultation with the reporting party and the organisation, the NCSC can also be involved in sharing information on the vulnerability with its constituency in order to limit further security risks arising from the vulnerability.

If the reporting of the vulnerability does not go as the reporting party expects, or if they would prefer not to report the vulnerability directly to the organisation, they can contact NCSC.[4] In this case, the NCSC can act as an intermediary where necessary.

The owner of the IT system is at all times responsible for the security of the system. Neither can the NCSC force the owner of the system to remedy a vulnerability, nor can it guarantee that the owner will not take legal action against the reporting party. As a result, the reporting party must take the aforementioned building blocks into account for organisations and reporting parties when searching for and reporting a vulnerability. A reporting party may expect the NCSC to do its utmost in order to have the vulnerability remedied and to treat the report confidentially. The NCSC does not share any personal data unless it is legally obliged to do so.

If possible, the NCSC will use the information obtained on vulnerabilities in consultation with organisations and reporting parties for further sharing the knowledge with the IT community. For example, it can do so by publishing part of the information, writing or updating a fact sheet or white paper, or by informing specific organisations.

- Depending on the organisation concerned and the nature of the vulnerability established, the NCSC will make an effort to bring the vulnerability to the attention of the organisation concerned. However, the owner of the IT system in question remains responsible for the system.
- Where possible and necessary, the NCSC will provide the organisation concerned with advice on how to remedy the vulnerability.
- The NCSC will treat reports confidentially and will not share the personal data of the reporting parties or receiving organisation without consent, unless it follows from a statutory obligation.
- Wherever possible, the NCSC will keep the reporting party informed of developments in the contact with the organisation and the remedying of the vulnerability.

4 See https://www.ncsc.nl/incident-response/responsible-disclosure-melding.html

- In cases where a report is made to the NCSC, the NCSC will try to bring the reporting party or potential reporting party and the organisation into contact with each other.

If a reporting party has found a vulnerability in a software product or a vulnerability that affects many different systems, for example, the reporting party can ask the NCSC to coordinate the remedying and disclosing of the vulnerability.

Together with the reporting party, partners, developers and/or software developers and other security teams, the NCSC will help to analyse, remedy or have remedied, coordinate and disclose the vulnerability in a controlled manner. All of this process takes place in close consultation with the reporting party who found the vulnerability.

A CVD policy attempts to strike a balance between the importance of disclosing vulnerabilities as quickly as possible, so measures can be taken, and the importance of developers as well as suppliers having sufficient time to remedy the vulnerability. For this process, the NCSC uses a standard term of 60 days between the report and the public disclosure. However, there may be circumstances in which it may be decided to extend or shorten this period.

The NCSC will only ever share information about the vulnerability with third parties after consultation with the reporting party. It is essential in this context that the NCSC cooperates and therefore shares information about the vulnerability with stakeholders so as to disclose a vulnerability in a coordinated manner. The NCSC will ensure in doing so that the right parties can work on remedying the vulnerability, help to limit any loss or damage and help to draw attention to the vulnerability that has been found.

Edwin van Andel

5. Communication and the disclosure process

Five years of practice has shown that clear communication is the cornerstone of a successful CVD process. There are points for attention on, during and after the CVD process.

Communication about the disclosure process

Publishing a CVD policy is a first step in communicating about the process. By publishing a policy publicly, reporting parties are invited to notify the organisation of any vulnerabilities found. On the one hand, the organisation can draw up conditions for the research that is done to discover vulnerabilities and the way that contact is sought. On the other hand, the organisation can commit itself to the principle that it will not file a complaint with the police if the rules of the policy are respected. This approach protects the position of the reporting party.

A CVD policy may be changed or updated at a later date. It is important to be clear about the changes in this regard. Reporting parties have an interest in knowing what has been changed and when. For example, clarifying changes can be done by including a date of publication at the beginning of the CVD policy, by describing a summary of changes under the CVD policy or by keeping an archive with old versions of the CVD policy.

The CVD policy can provide guidelines on how to communicate during the process, such as by indicating regular updates via email or a web portal. In addition, the CVD policy can describe how a reporter can be acknowledged by mentioning them in the event of an update, admission to a hall of fame or any other form of reward.

Communication during the disclosure process

A reporting party initiates a CVD process by sending a message to the organisation. In this message, the reporting party gives a clear description of the vulnerability discovered. Important elements are the IP address or URL of the affected system and the necessary steps for reproducing the vulnerability.

It is important for the organisation to communicate clearly to the reporting party so expectations about the process are clear. It can already do so by sending an acknowledgement of receipt (automated or otherwise) that contains an indication of the term within which an initial or subsequent substantive response will be sent.

An indication of a solution period can be given in a CVD policy. It is also possible to leave this period open and to give an initial indication of the term after assessing the content of the report. It is advisable to be clear as soon as possible about the period within which a solution can be achieved. In this way, the reporter knows when an outcome may be expected.

It may be possible in some cases that a publication date is already clear to the reporting party; for example, because of a presentation at a conference or because the reporting party has fixed their own term. In this case, it is still important that the reporting party communicates this timeline clearly, states it as early as possible and is clear about the possibility/impossibility of postponing this date.

A reporting party is often someone outside the organisation, who does not have any insight into the internal processes that can be triggered by a report. Organisations can keep the reporting party informed about the developments in the process through regular updates. This approach makes it clear to a reporting party that a solution is being worked on. Where necessary, an organisation can request clarification or to test a solution during the process.

If an organisation is unable to meet the initial resolution deadline, it can be discussed with the reporter to postpone it. Regular communication can make this situation clear to a reporter at an earlier stage.

The main intention of CVD is to mitigate the vulnerability, but 'full disclosure' of the vulnerability is always an option for a reporting party if it feels that the process will take too long. This measure is the proverbial 'big stick' available to the reporting party. Naturally, this situation must be prevented as much as possible.

Communication after the disclosure process

Many possible reasons exist why a reporting party might look for vulnerabilities and then report them to organisations via the CVD process. For a large number of reporting parties, an important incentive is (public) recognition.

Reporting parties receive public recognition via a thank you in an update or entry into a hall of fame. However, the need for public recognition does not apply to all reporting parties; some in fact do not want to be known to the public. In case of communication by the organisation, it is therefore advisable to obtain the consent of the reporting party for naming them.

In addition, reporting parties can also decide to communicate about a report after completion of the CVD process. For example, the reporting party can describe the discovery process or warn others about the vulnerability. A reporter may decide to submit the publication to an organisation for informational purposes. As the CVD process is in principle completed after the removal of the vulnerability, the reporting party is subsequently free to communicate about it, unless additional agreements are made in the policy or during the process.

Communication about the disclosure process

- Publication of the CVD policy on the website
- Be clear about restrictions (see chapter 6 for diferent approaches)
  - Restrictions in investigative methods
  - Guidelines about communication
  - Guidelines about possible rewards: Hall of fame, financial reward, t-shirt, etc.
- Be clear about any updates to the CVD policy, including the date of changes

Communcation during the disclosure process

- Reporter contacts organisation about a discovered vulnerability.
- Organisation manages expectations, such as the response time for a first technical response
- Organisation and reporter provide clarity to each other about expected resolution period
- Organisation frequently provides a (process) update
- Where necessary, reporter and organisation discuss contacting other relevant organisations

Communication after the disclosure process

- Discuss (public) recognition and reward of the reporter
- Arrange how information about the vulnerability will be published, such as the research phase or informing other organisations

Zawadi Done

6. Examples of Coordinated Vulnerability Disclosure policy

There are many different forms of policy texts on Coordinated Vulnerability Disclosure. As the published CVD policy acts as a signpost to potential reporting parties, make sure that the form of this policy is in line with the policy and strategy of the organisation.

The following elements are important in a CVD policy:
- contact method for secure communication;
- preconditions for reporting parties;
- clear expectations for handling a report;
- method for rewarding a report;
- version number and date of latest revision.

Below are three examples: Many organisations in the Netherlands have drawn from the basic example of ResponsibleDisclosure.nl. Other organisations include additional preconditions, see the policy of Fox IT. Still other organisations apply a freer format to align with their target audience, see the policy of Bits of Freedom.

ResponsibleDisclosure.nl

At the Acme Corporation, we consider the security of our systems a top priority. But no matter how much effort we put into system security, there can still be vulnerabilities present.

If you discover a vulnerability, we would like to know about it so we can take steps to address it as quickly as possible.
We would like to ask you to help us better protect our clients and our systems.

Please do the following:

- E-mail your findings to cert@example.com. Encrypt your findings using our PGP key to prevent this critical information from falling into the wrong hands,
- Do not take advantage of the vulnerability or problem you have discovered, for example by downloading more data than necessary to demonstrate the vulnerability or deleting or modifying other people's data,
- Do not reveal the problem to others until it has been resolved,
- Do not use attacks on physical security, social engineering, distributed denial of service, spam or applications of third parties, and
- Do provide sufficient information to reproduce the problem, so we will be able to resolve it as quickly as possible. Usually, the IP address or the URL of the affected system and a description of the vulnerability will be sufficient, but complex vulnerabilities may require further explanation.

What we promise:

- We will respond to your report within 3 business days with our evaluation of the report and an expected resolution date,
- If you have followed the instructions above, we will not take any legal action against you in regard to the report,
- We will handle your report with strict confidentiality, and not pass on your personal details to third parties without your permission,
- We will keep you informed of the progress towards resolving the problem,
- In the public information concerning the problem reported, we will give your name as the discoverer of the problem (unless you desire otherwise), and
- As a token of our gratitude for your assistance, we offer a reward for every report of a security problem that was not yet known to us. The amount of the reward will be determined based on the severity of the leak and the quality of the report. The minimum reward will be a €50 gift certificate.

We strive to resolve all problems as quickly as possible, and we would like to play an active role in the ultimate publication on the problem after it is resolved.

Fox-IT

At Fox-IT, we consider the security of our systems, our network and our products, of utmost importance. Despite the great care we take regarding security, weak points can still remain. If you have found such a weakness, we would like to hear about it as soon as possible so that we can take appropriate measures as quickly as possible.

Weak points can be discovered in two ways: you can accidently come upon something during the normal use of a digital environment, or you can explicitly do your best to find them.

Our responsible disclosure policy is not an invitation to actively scan our business network to discover weak points. We monitor our business network ourselves. This means that there is a high chance that a scan will be detected, and that an investigation will be performed by our Security Operation Center (SOC), which could result in unnecessary costs.

You are, however, invited to actively search for vulnerabilities in our products in an offline non-production environment and to report your findings to us. Our responsibility to our customers means that our intention is not to encourage hacking attempts on their infrastructure; however, we would like to hear from you as quickly as possible if vulnerabilities are found, so that we can resolve them adequately.

We would like to work with you to better be able to protect our customers and our systems.

We ask that you:

- E-mail your findings as quickly as possible to security-alert@fox-it.com.
- Do not abuse the vulnerability; for example, by downloading, editing or deleting data. We will always take your report seriously and investigate any suspicions of a vulnerability, even without proof.
- Do not share the problem with others until it has been resolved.
- Do not make use of attacks on physical security, of social engineering or hacking tools, such as vulnerability scanners.
- Give adequate information for the problem to be reproduced so that we can resolve it as quickly as possible. Usually, the IP address or the URL of the affected system and a description of the vulnerability are enough, although more information might be necessary for more complex vulnerabilities.

What we promise:

- We will respond to your report within three business days, with our evaluation of the report and an expected resolution date.
- We will handle your report confidentially, and will not share your personal information with third parties without your permission. An exception to this is the police and judiciary in the event of prosecution or if information is demanded.
- We will keep you informed of the progress of the solution to the problem.
- In communication about the reported problem, we will state your name as the party that discovered the problem, if you wish.
- It is unfortunately not possible to guarantee in advance that no legal action will be taken against you. We hope to be able to consider each situation individually. We consider ourselves morally obligated to report you if we suspect the weakness or data are being abused, or that you have shared knowledge of the weakness with others. You can rest assured that an accidental discovery in our online environment will not lead to prosecution.
- As thanks for your help, we offer a reward for every report of a security problem that is not known to us. We determine the value of the reward on the basis of the seriousness of the breach and the quality of the report.

We strive to resolve all problems as quickly as possible, to keep all involved parties informed and we would like to be involved in any publication about the problem once it is resolved.

With thanks to Floor Terra for his sample text in Dutch on http://responsibledisclosure.nl

Bits of Freedom

Our dependence on digital infrastructure is ever increasing. This applies to society as a whole, but also to ourselves. It is therefore our opinion that governments and organisations (including ours) should strongly commit to securing our digital infrastructure. We do realise that, in spite of our best intentions and greatest care, vulnerabilities may exist in our systems. If you do happen to find one of these weaknesses, we would love to hear from you so we can resolve the issue.

What we expect from you

- When you are investigating one of our systems, bear in mind the proportionality of the attack. There is no need to demonstrate that when you subject our website to the largest DDos-attack in the history of the internet, the site may become unreachable. We know that. We also understand that if you drive a bulldozer into our office, you will probably be able to snatch one of our laptops.
- This principle of proportionality is also relevant when demonstrating the vulnerability itself. You should not inspect or modify more data then strictly necessary in order to confirm the validity of your finding. For instance, if you are able to modify our homepage, just add a single non-controversial word to it instead of taking over the entire page. If you can obtain access to a database, it suffices to show us a list of the tables that are in there, or perhaps the first record in one of these tables.
- A vulnerability in one of our systems should be reported as soon as possible by sending an email to security@bof.nl. Preferably you would encrypt your message using OpenPGP. Please provide enough information so we can reproduce and investigate the issue.
- The public OpenPGP key for security@bof.nl
- You will not share your knowledge of the vulnerability with other parties as long as we have not addressed the issue and we are still within a reasonable timeframe since you reported the issue.
- You will delete all confidential information you have obtained during your investigation as soon as we have resolved the vulnerability.

What you can expect from us

- We will respond to your report within three days in a detailed manner. We will include an estimate of the time we will require to address the issue. Of course, we will regularly keep you posted on our progress.
- We will resolve the vulnerability as soon as possible. Here too, proportionality is important: the amount of time required to fix a vulnerability depends on several factors, among which the severity and the complexity of the issue at hand.
- When you follow the guidelines that are laid out here, we will not take legal action against you regarding your report.
- It is important to us to credit you for what you did - if you wish. We will mention your name in a publication regarding the vulnerability only if you agree to this.
- As a thank you for helping us in better protecting our systems, we would like to reward every report of a vulnerability that was unknown to us at the time. The reward will depend on the severity of the vulnerability and the quality of the report.
- Should you find a vulnerability in third party software that we use and that vulnerability is covered by a bug bounty program, we will not try to claim this bounty; you should.

Version 1.0 of 23 June 2017.

Publication
Nationaal Cyber Security Centre (NCSC)
PO Box 117, 2501 CC The Hague,
The Netherlands
Turfmarkt 147, 2511 DP The Hague,
The Netherlands
+31 70 751 5555

More information
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

Photography
Tobias Groenland |
hackershandshake.com

October 2018