NASK Cyber POLICY

Coordinated Vulnerability Disclosure (CVD)

Summary of the session “Together-safer, stronger, smarter”

Introduction

Ladies and Gentlemen,

It is my pleasure to present to you a publication summarizing the international session "Together-safer, stronger, smarter". The event, attended by international cybersecurity experts, was organized by NASK National Research Institute and took place on October 21, 2021.

The meeting was an opportunity not only to exchange experience and good practices, but to strengthen cooperation between NASK and European CVD experts. The session gathered representatives from national as well as international institutions involved in cyber security.

During the meeting, speakers presented national approaches, experiences and good practices in the area of coordinated vulnerability disclosure. All experts emphasized the important role of positive hackers and other entities (vendors, suppliers) informing about vulnerabilities in increasing the level of cyber security. Given the potential impact of these groups on security of ICT systems, devices and processes, it seems reasonable to amend current or introduce new regulations in order to ensure the immunity of all stakeholders involved in CVD process from criminal liability.

It is also necessary to establish frameworks and structures for the process of coordinated disclosure of vulnerabilities and to adopt clear, transparent rules of cooperation between all stakeholders.

Below you will find a summary of the different solutions presented by our colleagues and representatives from NCSC the Netherlands, BSI Germany and NBU Slovakia, CCB Belgium.

I wish you enjoyable reading and inspiration in your approach to CVD.

Krzysztof Silicki

NASK Deputy Director
Director for Cybersecurity and Innovations

European regulations

On December 16, 2020. The European Commission presented a new cybersecurity package, part of which, in addition to the new Cybersecurity Strategy and the Critical Entities Resilience Directive, is a proposal for a Directive on measures for a high common level of cyber security across the European Union – the so-called NIS 2 Directive.

Coordinated disclosure of information on vulnerabilities is an important issue, so the European Commission decided to include this process in the NIS 2 Directive proposal. In Article 6, the European Commission required each Member State to designate a national-level CSIRT to act as a coordinator in the vulnerability disclosure process and a trusted intermediary to facilitate interactions between the notifier/reporter and the manufacturer/producer or provider/supplier of ICT products or services. Adopting this approach will significantly strengthen the role of the CSIRT in the process of building public-private partnerships in cybersecurity.

On October 9, 2018, ENISA together with the National Cyber Security Center (NCSC, The Netherlands) presented a guideline for a coordinated process for disclosing vulnerabilities – Coordinated Vulnerability Disclosure: The Guideline. The document is the result of 5 years of cooperation between companies and the ICT community, government institutions, NCSC, as well as with law enforcement agencies – the Dutch police and prosecutors.

CVD – experiences of European countries. Summary of the closed session “Together-safer, stronger, smarter”.

On the 21st of October 2021, NASK National Research Institute hosted an international closed session “Together – safer, stronger, smarter”. The event was organized as part of the SECURE, one of the oldest conferences on IT security in Poland. For the fourth time representatives of national and international institutions dealing with cyber security met together to share knowledge, challenges and good practices.

This year the topic of the closed session was the CVD process. Presentations about national experiences were made by speakers from Belgium, Slovakia, the Netherlands and Germany. In addition, experts from Romania, Czech Rep. and Poland took part in the discussion.

Slovakia was represented by the National Security Authority (NBU). It’s expert talked about the motivation for creating a national CVD policy, the current state, as well as challenges for the future. Until recently, there was no national policy for coordinated vulnerability disclosure in Slovakia. Only in 2019 National Cyber Security Centre SK-CERT has developed guidelines on CVD. The document contains recommendations for vulnerability reporters, organizations, as well as cyber security authorities.

The Netherlands were represented by the National Cyber Security Centre (NCSC) expert, who presented: Coordinated Vulnerability Disclosure: The Guideline. It provides guidance for the CVD process for reporting, receiving institutions and reporting parties. It also addresses the role of the NCSC, areas of responsibility, and communication before, during, and after the disclosure process.

The document is the result of 5 years of cooperation between companies and the ICT community, government institutions, the NCSC, as well as with law enforcement agencies – the Dutch police and the public prosecutor’s office.

The presentation of representatives from the Federal Office for Information Security (BSI) from Germany dealt with more specialized issues related to the handling of vulnerabilities detected by CVD on the client side.

The experts raised the issue of communicating security messages to end users, as well as the problem of inconsistencies in security instructions from various vendors. They also presented CSAF 2.0 standard, which is designed to help automate the process of providing security information to both vendors and customers.

Center for Cyber Security Belgium (CCB) presented national approach to the CVD process. It is based on accession agreement between parties. There are also national guidelines which are included in Belgium Cybersecurity Strategy. CCB is working on the proposal of legal framework aimed to assure safety of the vulnerability reporter.

SLOVAKIA
National Security Office (NBU)

CVD PROCESS IN SLOVAKIA

Motivation

As the entire cyber security community, we are facing a huge increase in the number of vulnerabilities in software, hardware, as well as services and processes. Exploitation of vulnerabilities being one of the more common means of attack, can lead to full access to an organization's resources, including data and information stored in its systems and servers.

Until recently, there was no uniform national policy on CVD in Slovakia. There was a lack of developed or defined policies for both vulnerability reporters and organizations. Filling this gap is crucial for the vulnerability management process. It will allow to detect them independently from standard methods such as conducting pen tests or regular monitoring.

Current Status

In 2019, the National Cyber Security Center SK-CERT has developed a non-normative document entitled "Vulnerability Reporting Guidelines". The document is divided into the following sections:

Document structure subsumes:

- purpose of the document,
- importance of CVD,
- definition of vulnerability,
- definition of CVE and CVSS,
- rules and recommendations for
  - reporters (ethical hackers, researchers, ordinary citizens),
  - organizations
  - cybersecurity authorities
- process map of CVD

The purpose of the document is to provide support to good hackers, researchers, as well as ordinary citizens who report vulnerabilities. The document also explains the importance of implementing the CVD process and it's benefits to reporters and organizations.

The rules for reporters outline how and where to report vulnerabilities and what activities are illegal. For those affected by a reported vulnerability, the document explains what they should have implemented and the appropriate response to a report. Cybersecurity authorities can find recommendations in the document, as well as guidance on developing CVD policies and processes or how to coordinate them.

Challenges

In 2 years, we have seen both good and bad practices in CVD. There are still many challenges ahead in this area. Examples include: Implementing recommendations for bug bounty programs, incorporating lessons learned from CVD reported vulnerability cases, and at the same time, promoting the implementation and development of the coordinated vulnerability disclosure process itself.

THE NETHERLANDS
National Cyber Security Centre (NCSC)

Guidelines for the Responsible Disclosure Process.

The beginning of CVD in the Netherlands

Society is increasingly digitalizing, which creates many new opportunities. At the same time, vulnerabilities in information systems pose a potential threat to users, and their exploitation can cause serious consequences. At the beginning of this decade, reports of vulnerabilities were not well received, and cybercriminals were eager to exploit existing vulnerabilities to attack public and private organizations.

However, attitudes have changed over time and many organizations have noticed the advantages of having knowledge of vulnerabilities in their systems. Companies declared that they were open to receiving information about vulnerabilities under the previously agreed terms.

The NCSC conducted a consultation, the results of which were published in 2013 as "Responsible Disclosure Process. Guidelines". Companies declared that they were open to receiving information about vulnerabilities under the terms they had developed.

The mechanisms developed provided the opportunity to report vulnerabilities in a transparent and secure manner for the reporter. At the 2016 EU High Level Meeting on Cybersecurity, 29 organizations reaffirmed the importance of policies to deal with vulnerabilities by signing a joint document.

Coordinated Vulnerability Disclosure: The Guideline

On October 9, 2018, ENISA together with NCSC presented a guideline on CVD – Coordinated Vulnerability Disclosure: The Guideline.

The guidelines include information on:

- The purpose of coordinated vulnerability disclosure
- Areas of responsibility
- Guidance for the receiving institution and the reporting party
- The role of the NCSC
- Communication before, during, and after the disclosure process.

Also included are examples of Dutch company announcements containing vulnerability disclosure principles.

Lessons learned in recent years

In recent years, it has become clear that reporting parties are willing to work under the terms of the CVD regulation developed by NCSC. Reports are provided directly or indirectly to the organization by reporting parties. The practice of responsible disclosure has shown that bona fide reporting parties (with good intentions) and vulnerable organizations have been able to work together and thus take the next step in enhancing the security of networks and information systems.

GERMANY
Federal Office for Information Security (BSI)

Automating vulnerability warnings using the CSAF framework, or how to bridge the gap between the CVD process and system owners?

Vulnerability handling

At the end of the Coordinated Vulnerability Disclosure (CVD) process, a security message is typically issued to inform customers of a product and the public about the vulnerability and possible remediation options. This is actually the beginning of the vulnerability handling process on the part of the vulnerable system's owner.

At this stage, the end user should follow the issued warning and perform the recommended actions (installing a patch, update or other countermeasures). As every environment is different, and installing an update can sometimes have far-reaching consequences, a prior risk assessment is advisable. To make such an assessment, analyze the details of the vulnerability described in the message.

Constantly searching for security messages for many different products and assessing their suitability is time consuming and requires a lot of effort. This is due, on the one hand to the fact that manufacturers use different channels to reach their customers and the public, e.g:

- email (often with a delay),
- alerts on a dedicated RSS feed (subscription required),
- website (sometimes with limited access).

On the other hand, security warnings are increasing in number, and it is usually not easy to verify that the products referred to in these communications are used in the area for which the customer is responsible.

Lack of consistency in message format

Another problematic issue is the lack of consistency in the vulnerability warnings issued. Messages that come from different sources usually differ significantly from each other in terms of formatting, file format, structure and quality of information. Therefore, automatic processing of the information contained in them is not possible or is possible only to a limited extent.

In turn, delegating staff to these tasks unnecessarily occupies the time of highly skilled professionals. Furthermore, manual handling of such alerts is not scalable as the number of vulnerabilities increases. In practice, customers often do not use security messages continuously and regularly and, as a result, do not implement them in time. They act only on an ad hoc basis, for example after media coverage of an issue or on the advice of a national CSIRT such as BSI.

Common Security Advisory Framework (CSAF) 2.0 standard

To address this issue, the international community has jointly developed an open standard under the auspices of the OASIS Open Foundation – Common Security Advisory Framework (CSAF) version 2.0. It is based on the JSON format, which will help automate the process on both sides – both issuers of alerts and their recipients.

Replacing the XML-based Common Vulnerability Reporting Framework (CVRF) 1.2, CSAF also defines the availability and distribution locations of security messages. CSAF 2.0 defines requirements for tools that use it. The authors hope that in a few months everyone will be able to easily compare and choose from various tools available on the market.

Because the process is automated, this tool can be applied across the software and hardware supply chain. Vulnerability information can be passed down the supply chain much faster. Furthermore, it also becomes possible to clearly identify that a specific vulnerability is not present in a product by using a VEX (Vulnerability Exploitability eXchange) profile.

Such a mechanism can help reduce false positives from security scanners and, more importantly, support the hotline by proactively informing the customer that the product is not vulnerable.

OASIS Technical Committee members have already begun implementing their security messages in the format required by CSAF, including Arista, Cisco, Red Hat, and Siemens, among others. BSI has already published the first CSAF document creation tool (Secvisogram) in its repository available on GitHub. More tools and guidance on how to use the standard will follow in the future.

The latest information about the standard and available open source tools can be found at https://csaf.io. If you have any questions, please contact TC or BSI at csaf@bsi.bund.de.

Belgium
Centre for Cyber Security Belgium (CCB)

The Centre for Cyber Security Belgium (CCB) promotes the adoption of coordinated vulnerability disclosure policies (CVD) for private and public entities. It has published guidelines and provides an example of policy. Without modification of the existing legal framework, those guidelines clarify the legal situation of the researchers when the organisation has adopted a CVD policy and attributes a role to the CCB (as national CSIRT) as a CVD coordinator by default even when there is no CVD policy in place.

Belgium approach to CVD

In Belgium, a CVD policy or a bug bounty is considered as a type of accession agreement, which is usually published on a website, outlining the contractual provisions between the responsible organisation and the researchers (accepted by them when they freely decide to participate in the policy).

Subject to compliance with the mutual obligations described in the policy, the adoption of such a policy implies an authorisation from the responsible organisation for the researchers to access or to try to access, with good intentions, the concerned IT systems to identify possible vulnerabilities or to provide any relevant information about the security of its IT systems. Therefore, the access or the attempt to access those IT systems by the researchers are lawfully, as long as the pre-determined rules of the CVD are met.

These rules should ensure, inter alia, the confidentiality of the information exchanged and provide a responsible and coordinated framework for any disclosure of discovered vulnerabilities. The term 'disclosure' does not necessarily mean that the vulnerability will be made public, but rather that the participant communicates it to the responsible organisation.

The participant is obliged to communicate the vulnerability to the responsible organisation, but the public disclosure of the vulnerability (by the participant or the organisation concerned) is optional and must be coordinated. If a vulnerability is not yet known and threatens to have a direct or indirect impact elsewhere, the organisation responsible must inform the CCB and the other organisations potentially concerned, even if it does not want the vulnerability to be made public.

The national CVD policy is a formal policy explicitly included in the National Cybersecurity Strategy and in the CCB Baseline Security requirements for the public sector. The CCB adopted, as an example for other organisations, a CVD policy for its website.

Security for vulnerability reporters – proposed legislation

In the context of the implementation of the EU whistle blowers directive, the CCB has also made some legislative proposals aimed to offer a safe harbour under predetermined conditions, to vulnerability reporter who, in certain circumstances, can fulfil the role of digital whistle blowers. The specific conditions suggested are:

- to have acted without fraudulent intent, nor intention to harm;
- to have informed the organisation responsible for the system, process or control, as soon as possible and at the latest at the time of reporting to the national CSIRT (CCB), of the discovery of a potential vulnerability;
- be able to prove the proportionate nature of their actions and research methods, with regard to the objective of improving the security of the system, process or control concerned;
- they have not publicly disclosed information about the discovered vulnerability without the prior agreement of the national CSIRT.


NASK
Cyber POLICY