What is the purpose of the Common Vulnerabilities and Exposures (CVE) systems from a security perspective?

October 30, 2023

Share

Context and objective of the blog post

In the Intrusion and Application Security team (called IAS for the rest of the post), we discover and publish vulnerabilities found in commercial products almost every year since 2015. This process is done with the Common Vulnerability and Exposure (CVE) system.

With time, we faced different kinds of issues as well as misunderstandings in the publishing process. Therefore, we decided to create a blog post, in the form of a FAQ, to:

1. Provide a better understanding of the CVE system.
2. Play to MythBusters with some CVE's related myths.
3. Be transparent and precise about the way we handle a vulnerability that we identify in software (web, mobile, desktop…).

💡 The content of this post is based on our experience and on the responsible disclosure process that we follow, with the previous help of the Excellium Services' CSIRT.

🌎 This process is public.

Some definitions

The following terms were used in this post:

- **Common Vulnerabilities and Exposures (CVE)**: System providing a reference method for publicly known information-security vulnerabilities and exposures (source).
- **Vulnerability**: Flaws in a computer system that weaken the overall security of the device/system (source). In this post we focused on flaws affecting software.
- **Exploit**: Information and/or piece of code allowing the leverage of the vulnerability.
- **CVE worldwide database**: Global registry of CVE records managed by the MITRE corporation (more information).
- **CVE identifier**: It is a string identifying, in a unique way, a vulnerability referenced in the CVE worldwide database.
  - Its format is "CVE-[Year]-[UniqueNumberInTheYear]"
    - Year: The "Year" portion is the year that the CVE ID was reserved or the year the vulnerability was made public.
    - UniqueNumberInTheYear: Unique identifier of the CVE in the year.
  - Example: CVE-2022–38481
- **Vendor**: Entity developing, selling, and maintaining the software affected by the identified vulnerability.
- **Vulnerabilities scanners**: Vulnerability scanners are valuable tools that search for, and report on what known vulnerabilities are present in an organization's IT infrastructure (source).
- **Computer Security Incident Response Team (CSIRT)**: A capability set up for the purpose of assisting in responding to computer security-related incidents (source).
- **IAS**: Intrusion and Application Security team of Excellium Services (homepage).
- **CERT-XLM**: CSIRT of Excellium Services (homepage).
- **Grace period**: Amount of time, in days, that we give to a vendor to create a patch for the vulnerability. It is fixed to around 100 days, and it is explicitly documented in the responsible disclosure process that we follow. In case of need by the vendor to implements a correct remediation, a vendor can ask to extend the grace period.
- **CVE request form**: Templated document containing all the information of a vulnerability. This document is intended to be sent to the vendor of the affected software.

Frequently asked questions

What is the CVE system and why does it exist?

The CVE (Common Vulnerabilities and Exposures) process is a standardized method for identifying and naming cybersecurity vulnerabilities. It provides a unique identifier for each vulnerability, along with a detailed description of the issue and information on how to mitigate the risk.

Almost all vulnerability scanners tools use the CVE worldwide database to identify vulnerable products. Therefore, it can help companies to identify products affected by vulnerabilities. This, even if the vendor of the product did not notify its clients.

🧾 Example of usage of CVE by a:

- Free vulnerability scanner.
- Commercial vulnerability scanner.

By using the CVE process, organizations can stay informed about potential security threats and take actions to address them before they are exploited by attackers.

How does the presence of CVE IDs relate to a software?

In 2023, we can say that if a product has no CVE registered in the CVE worldwide database, then it is strongly suspicious… Indeed, products are affected by vulnerabilities over time, and it can be expected.

😉 Myth busted –> *No software is 100% secure!*

The presence of CVEs on a product demonstrates the capability and awareness of a vendor regarding the security of its products. It shows that the vendor has a process to:

1. Receive notification of vulnerabilities.
2. Handle and remediate them.
3. Communicate with the client and partners to warn them and help them to patch.

📡 It is an explicit marker and signal of:

1. Maturity from a cybersecurity perspective.
2. Honesty in the sense that the vulnerabilities are not "*hidden under the carpet!*"
3. Control over the security posture of your products.
4. Capabilities of reaction if a vulnerability is discovered on a product.

📍 As an example of companies, for which, the presence of CVE on their products has not broken the business model as well as trust from their clients, we can take (April 2023):

1. The company Microsoft with around **9500** CVE on their product.
2. The company Zoho with around **418** CVE on their product.
3. The company Ivanti with around **70** CVE on their product.
4. Other companies on this page.

The CVE descriptions can be a good indicator to see how a product vendor considers the security aspects:

- ❌ If the different CVE states that the vendor *did not reply to CSIRT notifications or refuse to patch*, it indicates that the vendor wants to "hide the vulnerability under the carpet" so it is best advised to avoid that vendor and their product line!
- ✅ If the different CVE mentions *a patch or a work around* then it is the reverse! Indeed, it indicates that the vendor takes and handles the security of their products seriously.

💡 This can even be leveraged as a differentiator from competitors, in the sense that vendors take the security of their product in a professional, transparent, and serious way.

What are our engagements as security vendor?

The consultants in charge of vulnerability assessments and incident response must follow ethical practices. They are committed to protect their clients and all the other users of software affected by vulnerabilities that put companies at risk.

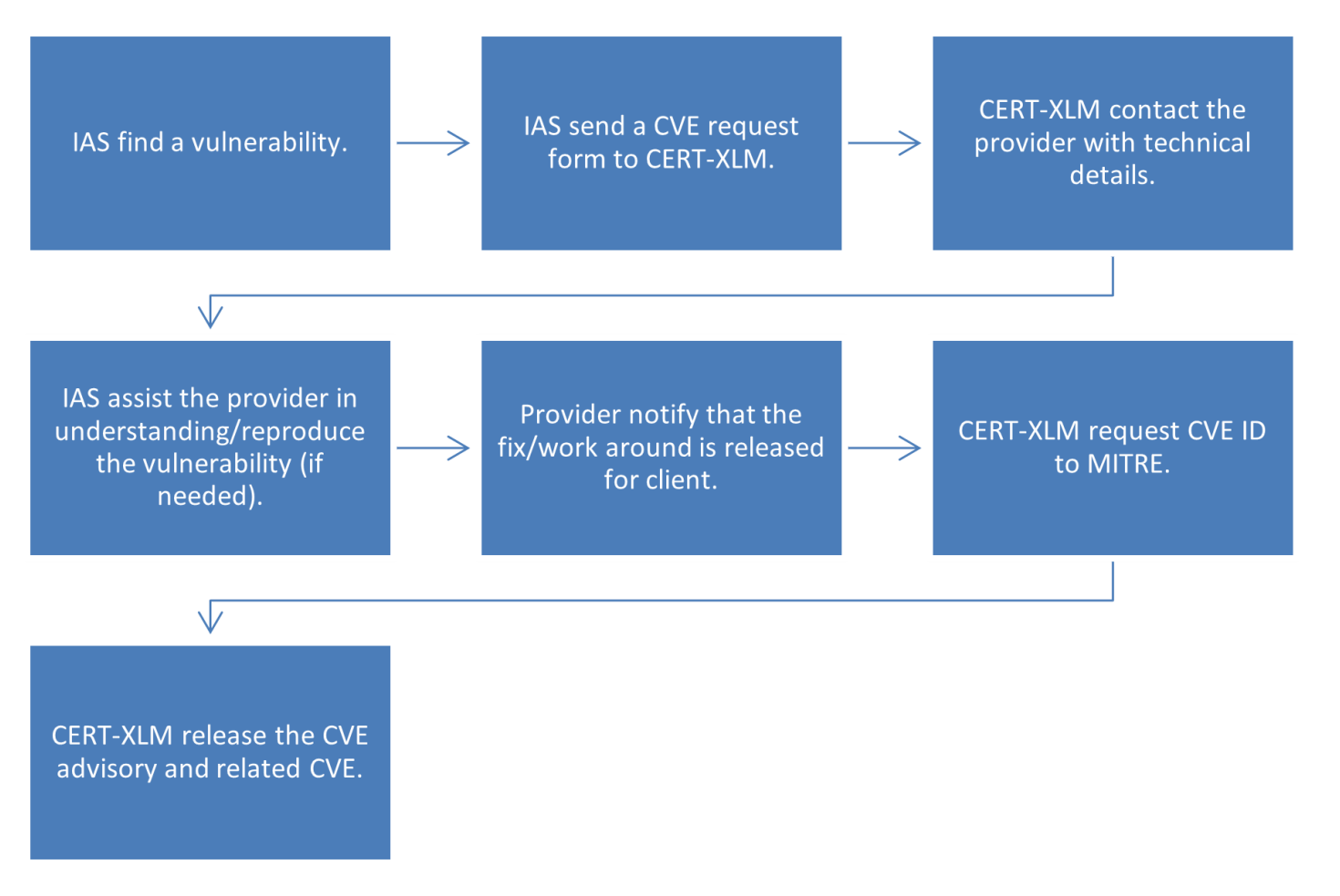
Intrusion & Application Security's members follow a mandatory code of conduct that describes how vulnerabilities found in commercial software should be handled.

CERT-XLM is an accredited team of Trusted Introducer (TI) and must follow with its Code of Practice and has a responsible disclosure policy for the handling of security vulnerabilities.

In which context a CVE process is initiated?

1. Excellium Services assesses a commercial software by working for a client, or directly for the vendor of the solution. Vulnerabilities can also be found outside of client engagements, while doing R&D on publicly available software (closed or open source).
2. A previously unknown vulnerability in discovered in the software.
3. The vulnerability is present in software default configuration.
4. The software is used by other clients which are consequently exposed to the same risks.

What is the general overview of this process?



What is shared by Excellium Services to the software vendor?

The CVE form shared privately with our client and the software vendor contains scoring, details and our recommendations to fix the issue. It needs to have details to help the vendor to fix the issues, but these details are never disclosed by Excellium to the public. In the form, there are two distinct sections with the elements that will be published and the elements that will not be published by Excellium.

When non-disclosure agreements (NDA) are signed by the client, Excellium Services and the software vendor, it means that the disclosure of application data, Personal Identifying Information (PII) or details about the infrastructure cannot be disclosed with third parties. Excellium Services always ensure that application data, PII and deployment details (IP addresses, URLs) are never disclosed to the software vendor during the CVE process.

However, NDAs are not meant to prevent Excellium Services to work with the vendor for the implementation of the fixes, nor prevent Excellium to publish a minimal set of information about the vulnerabilities and the CVE process history (more below in the following section).

What is published by Excellium Services?

The CVE ID and the associated general information (as described hereafter) are published on Excellium Services' web site when the vulnerability is fixed, or the 90-days period is due (either comes first).

1. The type of vulnerability like "*The application is prone to reflected Cross-site Scripting (XSS) attack in several features. This vulnerability allows an attacker to perform action on behalf of the users and exfiltrate data.*"
2. The severity of the vulnerability using the CVSS v3 scoring system.
3. The range of versions affected.
4. The associated patch or work around to apply.
5. The "*Vulnerability Disclosure Timeline*" with all communication events.

🧾 Example of CVE advisory that we published.

What is NOT published by Excellium Services?

There are a lot of misconceptions around the level of information that is disclosed at the end of the CVE process. Depending on the context, security researchers may decide to disclose more than necessary information.

At Excellium Services, we have chosen to never share detailed information so it could not endanger users of vulnerable softwares. Companies that use vulnerable softwares may not be able to patch it for numerous reasons (unaware of the issue, lack of time, financial or technical constraints…). Consequently, the following items are never published by Excellium:

- The name of the client (when the vulnerability is discovered in the context of an assessment)
- The details of the vulnerability (location and technical details of the exploitation)
- The detailed impact of the vulnerability
- People names and content of messages exchanged with the software vendor
- An exploit for anyone to use and abuse the vulnerability

What are the general hiccups of the CVE process?

Despite the clear benefits of the CVE process, some organizations may be hesitant to participate due to concerns about the potential impact on their image.

If a software vendor attempts to forbid Excellium Services from publishing CVEs, it indicates that the vendor is not confident about the security of their products. Clients should investigate this further to ensure the security of their systems.

The most common blocking points of the publication process are presented below.

The vendor does not answer to solicitations from our CSIRT

The CERT-XLM will try to find a more direct channel (like phone). If no reply is obtained after several attempts, they wait until the end of the grace period and publish the CVE indicating the absence of reply of the vendor in the CVE's "Vulnerability Disclosure Timeline".

The vendor disputes the nature of vulnerability for the reported problem

In this case, we try to explain the vulnerability and the risk from a technical perspective, this, in a more didactic possible way with proof of concept, technical call…

If after all our attempts, they refuse to fix the vulnerability, then CERT-XLM will wait until the end of the grace period and publish the CVE indicating the posture of the vendor in the CVE's *"Vulnerability Disclosure Timeline"*.

📍 If during an exchange with the vendor, we discover that the vulnerability "is a real built-in feature", then we can decide to cancel the CVE process. The vendor indicates explicitly the risks of using this feature in the documentation.

🛡️ In all cases, we ensure that an identified vulnerability will never be put "under the carpet" by a vendor!

The vendor needs more time to fix the issue

When an honest and transparent communication channel is established, we wait for the time the vendor needs to release an effective patch. We can test the patch to ensure that it is effective if the vendor asks for our assistance.

📍 To help the vendor, the IAS team always provides detailed technical advice, to fix the identified vulnerability, in the CVE request form intended to the vendor.

The vendor threatens to take legal action in case of publication

Some vendors may react defensively or even threaten legal action when presented with vulnerability reports. This response can be attributed to fears of reputational damage, financial loss, and potential exploitation of the vulnerability by malicious actors. Their reasons are usually one or more of the followings:

1. Reputational Damage: Publicly disclosed vulnerabilities can tarnish a vendor's reputation and erode customer trust, which may negatively impact sales and brand loyalty.
2. Financial Concerns: Vendors may worry that acknowledging vulnerabilities publicly could lead to financial liabilities, including potential legal action or loss of business.
3. Timely Mitigation: Vendors may want to control the disclosure process to ensure they have adequate time to develop and deploy patches before the vulnerability becomes widely known.

Despite the challenges, responsible vulnerability disclosure remains paramount for several reasons:

1. User Protection: Promptly addressing vulnerabilities protects users from potential exploitation and safeguards their sensitive data.
2. Collaborative Security: By embracing responsible disclosure, vendors can foster a collaborative relationship with the cybersecurity community, leading to stronger products and improved security practices.
3. Regulatory Compliance: Emphasizing responsible disclosure aligns with industry standards and can help vendors meet compliance requirements.
4. Public Perception: A vendor's commitment to addressing vulnerabilities responsibly can enhance its reputation as a security-conscious organization.

🤝 In such situations, Excellium always try to discuss with the vendor to understand the problem and find a positive solution. However, in all case, threats will not prevent the publication of the CVE.

What can you do as a vendor to be prepared in case of discovered vulnerabilities?

Creating an environment that encourages responsible vulnerability disclosure requires collaboration and understanding from all parties involved. To strike the right balance, the following steps are essential:

1. Clear Policies: Vendors should establish clear vulnerability disclosure policies, detailing how researchers can report vulnerabilities and how they will be acknowledged and addressed.
2. Bug Bounty: When a high level of confidence is reached and the vendors have transparent process, implementing a bug bounty program can incentivize researchers to report vulnerabilities responsibly while protecting them from potential legal consequences.
3. Communication: Open and respectful communication between vendors and researchers fosters trust and cooperation.
4. Acknowledgment and Recognition: Vendors should recognize and appreciate the contributions of researchers who responsibly report vulnerabilities, emphasizing the shared goal of enhancing cybersecurity.

Conclusion

In summary, CVEs are a crucial tool for maintaining the security of software systems. They promote transparency, improve the quality of software, benefit the entire security community and are widely adopted by the security industry. We strongly recommend that organizations take CVEs seriously and use them as part of their security strategy.

Authors

- Julien EHRHART
- Dominique RIGHETTO

Do you have any questions? Would you like to know more about the Common Vulnerabilities and Exposure (CVE) systems? Contact our experts!

Name *

First | Last

Company *

Phone Number *

Email *

Comment or Message *

Submit

Cyber Blog Post | Common Vulnerabilities And Exposures, CVE, Cyber Incident, Cyber Solutions, Cyber-Attacks, Cybersecurity, Excellium Services Belgium, Excellium Services Luxembourg, IT Security, Security, Thales

Recent Posts

- The Necessity of Cyber Crisis Exercises
- The Art of Password Spraying: A Comprehensive Analysis
- Common client-side vulnerabilities of web applications

Categories

- Advice
- Consulting
- Cyber Blog Post
- General
- Newsletter
- PR
- The Cyber Blog Times
- Uncategorized

Search

Search …