

Dicas: Como reportar uma
falha?

#0day #CVE #BugBounty

Joas Antonio

Detalhes

- Esse documento foi criado para ajudar pesquisadores de segurança da informação a reportar suas vulnerabilidades e obter suas CVEs;
- Espero que ajude de alguma forma a reportar seu 0day ou alguma vulnerabilidade em programas de Bug Bounty;

Meu LinkedIn: <https://www.linkedin.com/in/joas-antonio-dos-santos/>

Como encontrar vulnerabilidades?

- Primeiramente, é necessário conhecer os vetores de ataque do ambiente que você está explorando, seja uma aplicação web, um Hardware ou um sistema operacional. Entender como ele funciona e quais são os principais vetores de ataque, que tipos de exploração de vulnerabilidade é comum e pegar algum recurso, algum plugin ou componente e procurar vulnerabilidades, seja a nível de aplicação ou até mesmo em baixo nível;
- Segundo, eu recomendo que procure programas de recompensa também, pois quando se tem algo para testar e aprimorar suas habilidades pode ser que você encontre vulnerabilidades e certamente ganhe uma recompensa;
- Terceiro, você pode testar os equipamentos que você tem em casa, seja um roteador por exemplo, e assim procurar vulnerabilidades neles;
- Eu recomendo que você foque e teste todas as possibilidades, muita das vezes uma vulnerabilidade pode levar a outra, por isso é sempre bom conhecer e saber mesclar todo tipo de vulnerabilidade para gerar um impacto maior;
- Explore banco de dados de vulnerabilidades como exploit-db e o próprio Mitre, pois você pode acabar melhorando uma PoC ou encontrando algo novo e mais crítico ainda;

Plataformas de Bug Bounty

- HackerOne
- Bugcrowd
- Intigrity
- Bug Hunt
- Hackaflag
- Yogosha
- Zeroday initiative
- Open Bug Bounty
- YesWeHack
- Cobalt.io
- Synack Red Team

Como eu sei que tenho um Oday?

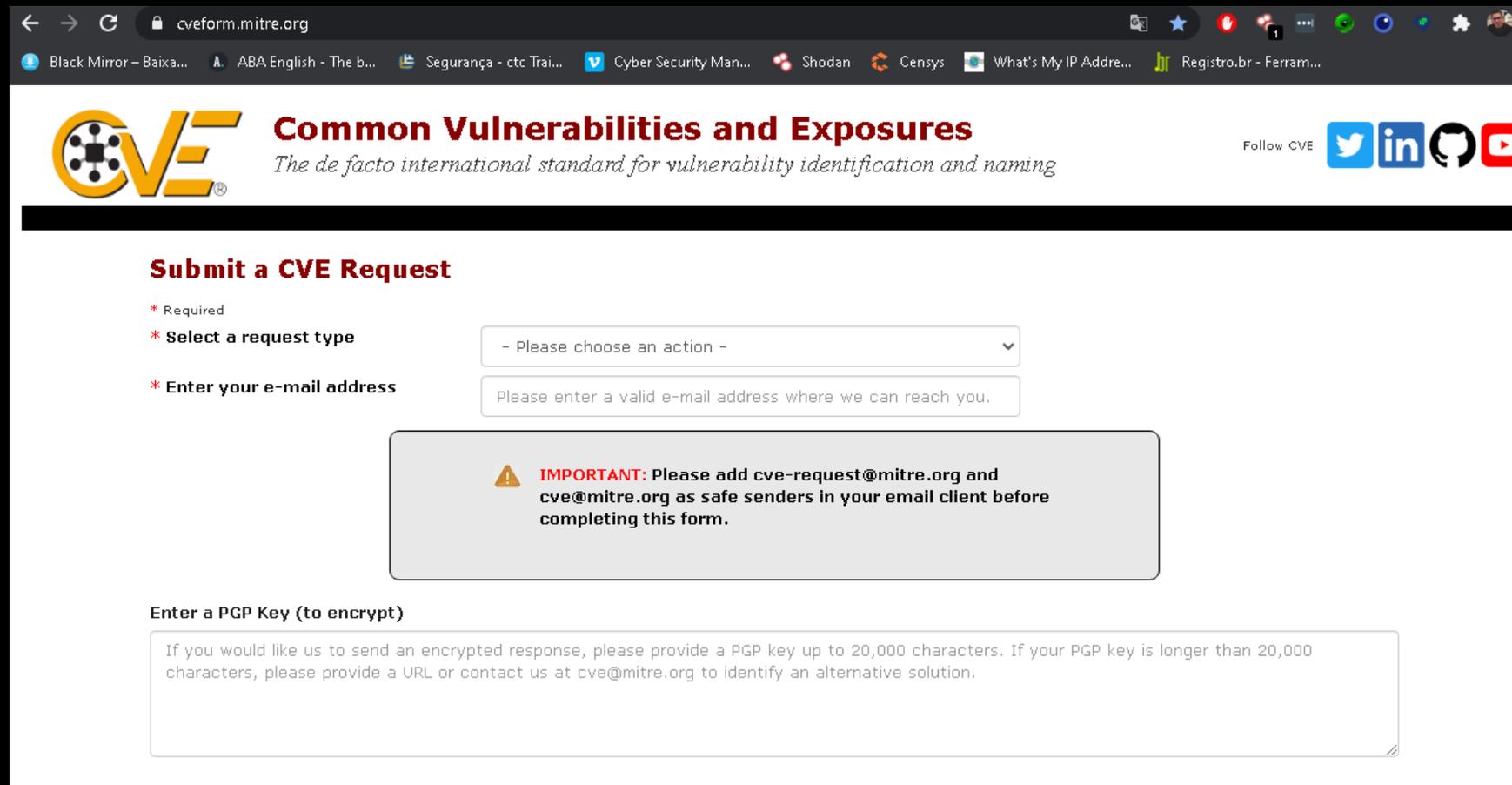
- Afeta algum produto? Algum componente que é utilizado por terceiros? Ou que afeta a versão de algum programa? Existe algum exploit da vulnerabilidade que você achou para esse produto específico? Existe alguma CVE Registrada? Consegue replicar essa vulnerabilidade em um ambiente específico ou em qualquer tipo de ambiente? Essa vulnerabilidade precisa ativar alguma configuração extra?
- Essas perguntas que você deve se fazer, as duas últimas é detalhes a mais, porém você tem um Oday respondendo pelo menos sim nas 4 primeiras perguntas;
- Mas em caso de dúvidas, reporte essa vulnerabilidade e espere a fabricante se pronunciar;

Como reportar para o Mitre e obter minha CVE?

- Dependendo do Report que você fizer, sua CVE pode ser gerada em pouco tempo, mas para isso você precisa ser bem objetivo no seu report e ter informações suficientes;
- Quer aprender a reportar? Segue o passo a passo nas próximas páginas;

Reportando sua vulnerabilidade: Acessando Site

- Acesse o site: <https://cveform.mitre.org>



The screenshot shows a web browser window with the URL `cveform.mitre.org`. The browser's address bar and tabs are visible at the top. The page header features the CVE logo on the left, the text "Common Vulnerabilities and Exposures" in a bold red font, and the tagline "The de facto international standard for vulnerability identification and naming" in a smaller, italicized font. To the right of the header are social media icons for Twitter, LinkedIn, GitHub, and YouTube, with the text "Follow CVE" above them.

The main content area is titled "Submit a CVE Request" in a bold red font. Below this title are two required fields, each marked with a red asterisk:

- * Select a request type**: A dropdown menu with the text "- Please choose an action -" and a downward arrow.
- * Enter your e-mail address**: A text input field with the placeholder text "Please enter a valid e-mail address where we can reach you."

Below the input fields is a grey-bordered box containing an important notice:

⚠ IMPORTANT: Please add `cve-request@mitre.org` and `cve@mitre.org` as safe senders in your email client before completing this form.

At the bottom of the form, there is a section titled "Enter a PGP Key (to encrypt)" followed by a text area containing the following text:

If you would like us to send an encrypted response, please provide a PGP key up to 20,000 characters. If your PGP key is longer than 20,000 characters, please provide a URL or contact us at `cve@mitre.org` to identify an alternative solution.

Reportando sua vulnerabilidade: Tipo de submissão

- Vamos selecionar no Select a Request Type: **Request a CVE ID**

Submit a CVE Request

* Required

* **Select a request type**

* **Enter your e-mail address**

- Please choose an action -

- Please choose an action -

Request a CVE ID

Request a block of IDs (For CNAs Only)

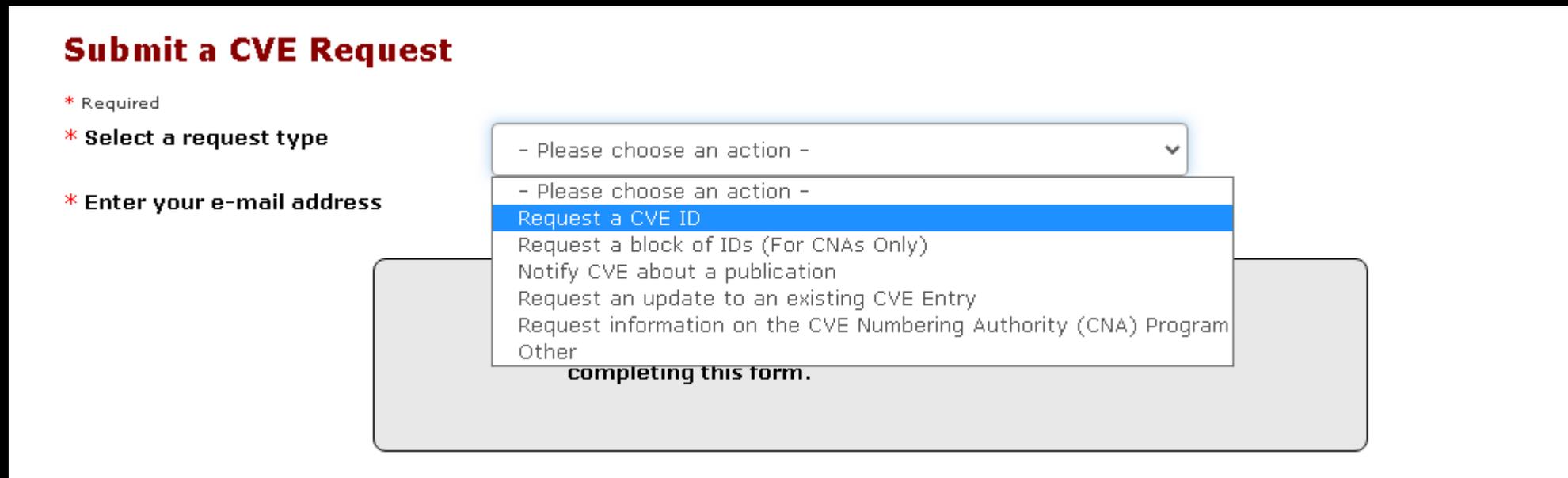
Notify CVE about a publication

Request an update to an existing CVE Entry

Request information on the CVE Numbering Authority (CNA) Program

Other

completing this form.

The image shows a web form titled "Submit a CVE Request". On the left side, there are three red asterisks indicating required fields: "* Required", "* Select a request type", and "* Enter your e-mail address". The "Select a request type" field is a dropdown menu that is currently open, showing a list of options. The first option is "- Please choose an action -" (disabled). The second option is "- Please choose an action -" (disabled). The third option, "Request a CVE ID", is highlighted in blue, indicating it is the selected option. Below the dropdown menu, there are several other options: "Request a block of IDs (For CNAs Only)", "Notify CVE about a publication", "Request an update to an existing CVE Entry", "Request information on the CVE Numbering Authority (CNA) Program", and "Other". At the bottom of the form, there is a text box with the text "completing this form.".

Reportando sua vulnerabilidade: Definindo E-mail

- Vamos selecionar no Enter your e-mail address: **Coloque seu e-mail que vai receber as notificações da CVE e etc...**

Submit a CVE Request

* Required

* Select a request type

* Enter your e-mail address

 **IMPORTANT:** Please add `cve-request@mitre.org` and `cve@mitre.org` as safe senders in your email client before completing this form.

 **IMPORTANT:** Once a CVE ID is assigned to your vulnerability, it will not be published in the CVE List until you have submitted a URL pointing to public information about the vulnerability. Without a public reference, the CVE ID will display as "RESERVED" in the CVE List. Please update CVE with a reference to the vulnerability's details as soon as possible. [See this FAQ](#) for more information.

Reportando sua vulnerabilidade: Quantas CVEs serão geradas

- Você pode definir o número de IDs necessário para sua CVE, caso sejam múltiplas vulnerabilidades que deseja reportar em um único componente, software ou sistema.

* Number of vulnerabilities reported or IDs requested (1-10) Do you need more than 10 IDs?

This page will automatically update to provide one request form for each of the CVE IDs requested.



Before submitting this request you should check whether the affected vendor is a CNA (see <http://cve.mitre.org/cve/cna.html>). Vulnerabilities in CNA products must be sent to the vendor in question. Also you should confirm that the vulnerability does not already have a CVE ID (see <http://cve.mitre.org/cve/cve.html>)

* I have verified that this vulnerability is not in a **CNA-covered** product.

* I have verified that the vulnerability has not already been assigned a **CVE ID**.

Reportando sua vulnerabilidade: CNA

- As CNAs são os responsáveis pela atribuição dos IDS da CVE e por manter essas informações e as publicar, dentro do escopo de cada organização, geralmente grandes empresas entram para controlar regularmente as CVEs que são atribuídas aos seus produtos;
- Consulte a lista de CNA, caso o fabricante esteja entre essas listas, reporte diretamente a eles;
- Se não, basta marcar a primeira caixa e caso também não tenha uma CVE atribuída, marque a segunda caixa;

* Number of vulnerabilities reported or IDs requested (1-10) Do you need more than 10 IDs?

This page will automatically update to provide one request form for each of the CVE IDs requested.



Before submitting this request you should check whether the affected vendor is a CNA (see <http://cve.mitre.org/cve/cna.html>). Vulnerabilities in CNA products must be sent to the vendor in question. Also you should confirm that the vulnerability does not already have a CVE ID (see <http://cve.mitre.org/cve/cve.html>)

* I have verified that this vulnerability is not in a **CNA-covered** product.

* I have verified that the vulnerability has not already been assigned a **CVE ID**.

Reportando sua vulnerabilidade: CNA

- As CNAs são os responsáveis pela atribuição dos IDS da CVE e por manter essas informações e as publicar, dentro do escopo de cada organização, geralmente grandes empresas entram para controlar regularmente as CVEs que são atribuídas aos seus produtos;
- Consulte a lista de CNA, caso o fabricante esteja entre essas listas, reporte diretamente a eles;
- Se não, basta marcar a primeira caixa e caso também não tenha uma CVE atribuída, marque a segunda caixa;

* Number of vulnerabilities reported or IDs requested (1-10) Do you need more than 10 IDs?

This page will automatically update to provide one request form for each of the CVE IDs requested.



Before submitting this request you should check whether the affected vendor is a CNA (see <http://cve.mitre.org/cve/cna.html>). Vulnerabilities in CNA products must be sent to the vendor in question. Also you should confirm that the vulnerability does not already have a CVE ID (see <http://cve.mitre.org/cve/cve.html>)

* I have verified that this vulnerability is not in a **CNA-covered** product.

* I have verified that the vulnerability has not already been assigned a **CVE ID**.

Reportando sua vulnerabilidade: Tipo de Vulnerabilidade

- Vamos definir um tipo de vulnerabilidade, caso não seja nenhuma da lista, clique em Other or Unknown e coloque o nome da vulnerabilidade;

Required

* Vulnerability type ⓘ

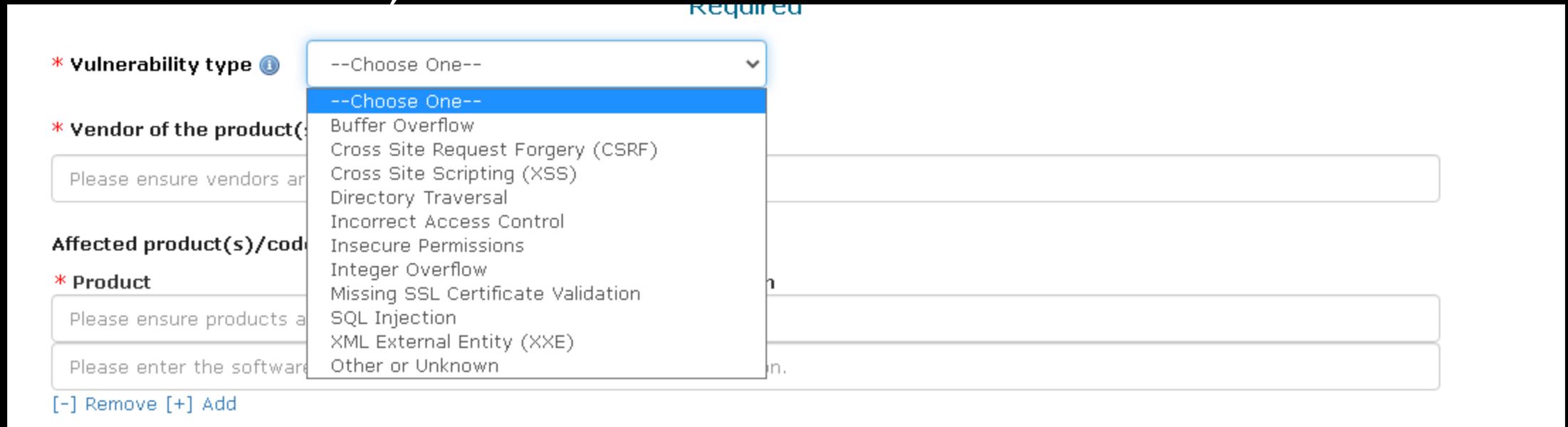
* Vendor of the product (Please ensure vendors are listed in the report)

Affected product(s)/code

* Product (Please ensure products are listed in the report)

Please enter the software name.

[-] Remove [+] Add



The image shows a web form for reporting a vulnerability. A dropdown menu is open for the 'Vulnerability type' field, which is marked as required. The dropdown contains the following options: --Choose One--, --Choose One-- (highlighted), Buffer Overflow, Cross Site Request Forgery (CSRF), Cross Site Scripting (XSS), Directory Traversal, Incorrect Access Control, Insecure Permissions, Integer Overflow, Missing SSL Certificate Validation, SQL Injection, XML External Entity (XXE), and Other or Unknown. The form also includes fields for 'Vendor of the product', 'Affected product(s)/code', and 'Product', each with a placeholder text. At the bottom, there are links for 'Remove' and 'Add'.

Reportando sua vulnerabilidade: Definindo Fabricante e Produto

- Agora vamos definir o Vendor (Fabricante) do produto, embaixo está um exemplo;
- Depois o produto que está sendo afetado e a versão dele, seja versão do firmware ou build dependendo da circunstância;

Required

* Vulnerability type ⓘ

Buffer Overflow

* Vendor of the product(s) ⓘ

Microsoft

Affected product(s)/code base ⓘ

* Product

Windows 10

* Version

10.0.18363 N/A compilação 18363

[\[-\] Remove](#) [\[+\] Add](#)

Reportando sua vulnerabilidade: Reconheceu a vulnerabilidade e Tipo de Ataque

- Ele vai perguntar se o Fabricante confirmou ou reconheceu a vulnerabilidade, caso você não tenha reportado para ele, coloque NO, mas recomendo você reportar;
- E o tipo de ataque você vai escolher, Local, Físico, Remoto ou caso nenhum desses, coloque outro;

Optional

Has vendor confirmed or acknowledged the vulnerability? Yes No

Attack type ⓘ

Impact ⓘ

- Code Execution
- Denial of Service
- Escalation of Privileges

Dropdown menu options:

- Choose One--
- Choose One--
- Context-dependent
- Local
- Physical
- Remote
- Other

Reportando sua vulnerabilidade: Reconheceu a vulnerabilidade e Tipo de Ataque

- Tipo de impacto que a vulnerabilidade causa, seja uma execução de código, negação de serviço ou escalar privilégios e outras vulnerabilidades;

Impact

- Code Execution
- Denial of Service
- Escalation of Privileges
- Information Disclosure
- Other

Reportando sua vulnerabilidade: Componente afetado e vetor de ataque

- Esse é um exemplo que eu fiz, claro não leve a sério é apenas para dar uma ideia, mas os componentes afetados é uma configuração, plugin, biblioteca, API e etc;

Has vendor confirmed or acknowledged the vulnerability? Yes No

Attack type ⓘ

Impact ⓘ

Code Execution Information Disclosure
 Denial of Service Other
 Escalation of Privileges

Affected component(s)

Afetando o componente Kernel32.DLL (EXAMPLE)
Affecting the Kernel32.DLL component

Attack vector(s)

Um invasor consegue executar código remoto no alvo, sobrescrevendo o EIP do Kernel32.DLL e injetando um Payload e (EXAMPLE)
An attacker can execute remote code on the target, overwriting the EIP of Kernel32.DLL and injecting a Payload and (EXAMPLE)

Reportando sua vulnerabilidade: Componente afetado e vetor de ataque

- O vetor de ataque é a forma como é explorada, como o atacante efetua o ataque, o que é explorado e etc...

Has vendor confirmed or acknowledged the vulnerability? Yes No

Attack type ⓘ

Impact ⓘ

Code Execution Information Disclosure
 Denial of Service Other
 Escalation of Privileges

Affected component(s)

Afetando o componente Kernel32.DLL (EXAMPLE)
Affecting the Kernel32.DLL component

Attack vector(s)

Um invasor consegue executar código remoto no alvo, sobrescrevendo o EIP do Kernel32.DLL e injetando um Payload e (EXAMPLE)
An attacker can execute remote code on the target, overwriting the EIP of Kernel32.DLL and injecting a Payload and (EXAMPLE)

Reportando sua vulnerabilidade: Descrição da vulnerabilidade

- Uma descrição da vulnerabilidade não precisa conter o exploit nem nada do tipo, só resumir o que se trata a vulnerabilidade e qual componente ele explora, lembre-se que a Prova do Conceito é algo a parte, quando sair a correção você pode postar em seu blog ou redes sociais e o CVE se torna um Identificador para auxiliar as outras empresas a corrigir tal vulnerabilidade identificada.

<http://cveproject.github.io/docs/content/key-details-phrasing.pdf>

Suggested description of the vulnerability for use in the CVE ⓘ

Buffer Overflow in Kernel32.DLL in Vendor Microsoft Windows 10 allow Attackers execute remote code on the target and escalate privileges, without the need for user interaction|

Discoverer(s)/Credits ⓘ

Joas Antonio

Reportando sua vulnerabilidade: Descrição da vulnerabilidade

- Uma descrição da vulnerabilidade não precisa conter o exploit nem nada do tipo, só resumir o que se trata a vulnerabilidade e qual componente ele explora, lembre-se que a Prova do Conceito é algo a parte, quando sair a correção você pode postar em seu blog ou redes sociais e o CVE se torna um Identificador para auxiliar as outras empresas a corrigir tal vulnerabilidade identificada.

Suggested description of the vulnerability for use in the CVE ⓘ

Buffer Overflow in Kernel32.DLL in Vendor Microsoft Windows 10 allow Attackers execute remote code on the target and escalate privileges, without the need for user interaction|

Discoverer(s)/Credits ⓘ

Joas Antonio

Reportando sua vulnerabilidade: Conclusão

- Após isso, as outras informações não são necessárias, mas recomendo que você coloque informações complementares se for necessário para detalhar mais a vulnerabilidade;
- Depois que você preencher as informações e obter sua CVE ela vai ficar reservada para depois ser divulgada;
- Conforme cada report realizado, você vai adquirindo mais skills para que sua CVE seja aprovada rapidamente, sem a necessidade de dar informações mais precisas;

CONCLUSÃO

- E se você quiser obter mais detalhes referente a carreira na área de bug bounty, eu desenvolvi um documento: <https://bit.ly/3hgypb4>
- Espero que esse documento ajude você de alguma forma, convido você entrar no meu perfil, pois lá tenho alguns artigos sobre Relatório, CVEs, Zeroday e etc;

Fique a vontade em me contatar, abraços!