How to report a vulnerability and generate its CVE?

Joas A. Santos

https://www.linkedin.com/in/joas-antonio-dos-santos

Como encontrar vulnerabilidades?

- É necessário conhecer a arquitetura do serviço, plataforma, tecnologia ou hardware que vai procurar suas vulnerabilidades;
- Entender como ele funciona e quais são os principais vetores de Ataque;
- Aderir programas de Bug Bounty pode te ajudar a gerar uma CVE, principalmente programas fechados ou exclusivos de uma tecnologia especifica Ex: Chrome, Firefox, Xaomi, Samsung, Meta e etc;
- Já pensou em bater um Nmap nos aparelhos da sua casa? Você pode testar os seus equipamentos e assim procurar vulnerabilidades neles, ex: Roteadores;
- Pratique suas habilidades em CVEs existentes, quem sabe contornar até mesmo uma remediação colocada pela fabricante (vendor)?

How to find vulnerabilities?

- It is necessary to know the architecture of the service, platform, technology or hardware that will look for its vulnerabilities;
- Understand how it works and what are the main attack vectors;
- Joining Bug Bounty programs can help you generate a CVE, especially closed or exclusive programs of a specific technology Ex: Chrome, Firefox, Xaomi, Samsung, Meta and others;
- Have you ever thought about hitting an Nmap on your home appliances? You can test your equipment and look for vulnerabilities in them, ex: Routers;
- Practice your skills on existing CVEs, maybe even bypass a vendor-placed remediation?

Como eu sei que tenho um 0day?

- O seu alvo é algum produto em especifico?
- Um Plugin?
- Um serviço?
- Uma biblioteca?
- Algum Framework ou CMS?
- Existe algum exploit da vulnerabilidade que você achou para esse produto em especifico?
- Existe alguma CVE Registrada?
- Essa vulnerabilidade afeta um ambiente especifico?
- Essa vulnerabilidade precisa ativar alguma feature?
- Qual impacto ela gera?

Os 0days elegíveis para CVEs, surgem de produtos desenvolvidos, Ex: Wordpress, Drupal, Apache2, Browsers, Drivers, Sistemas operacionais e entre outros;

Mas em caso de dúvidas, reporte essa vulnerabilidade e espere a fabricante se pronunciar;

How do I know I have a 0day?

- Is your target a specific product?
- A Plugin?
- A service?
- A library?
- Any Framework or CMS?
- Are there any exploits of the vulnerability you found for this specific product?
- Are there any Registered CVEs?
- Does this vulnerability affect a specific environment?
- Does this vulnerability need to enable some feature?
- What impact does it generate?

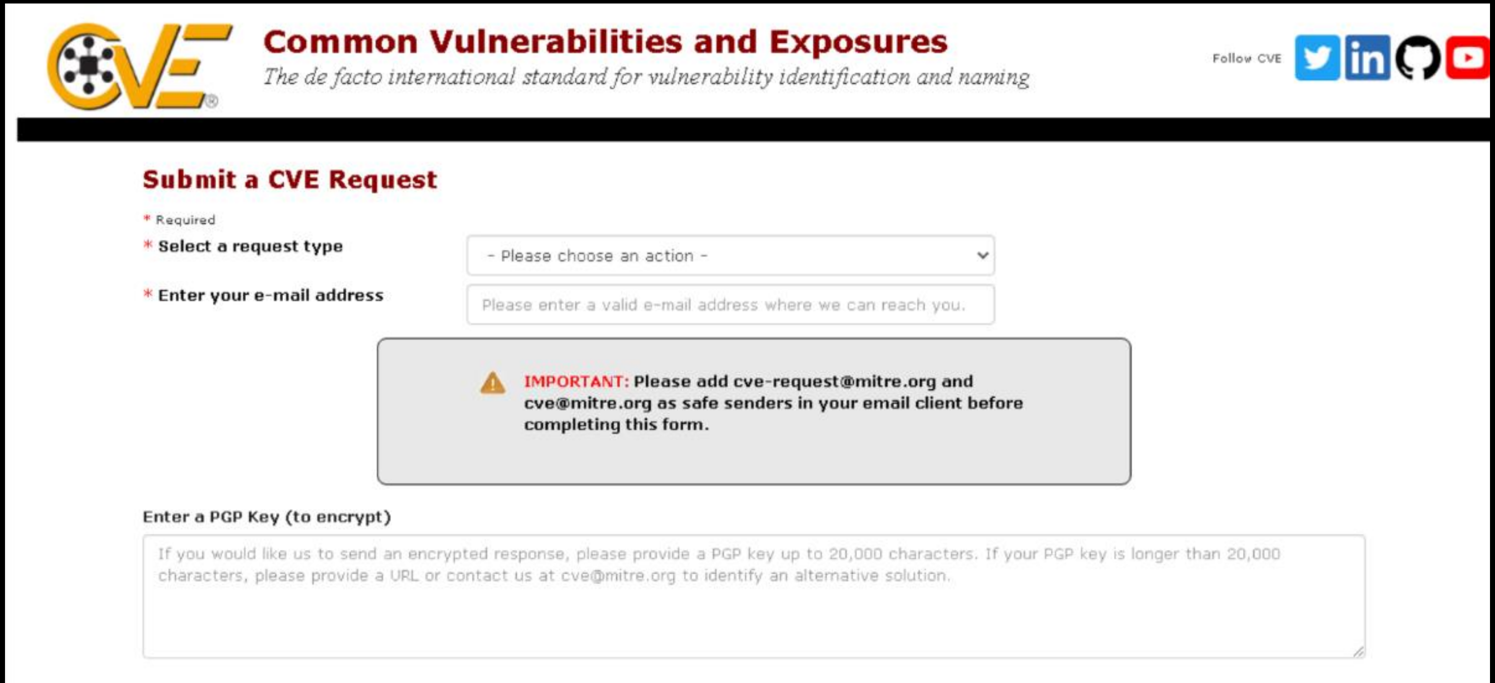
The 0days eligible for CVEs arise from developed products, Ex: Wordpress, Drupal, Apache2, Browsers, Drivers, Operating Systems and others;

But in case of doubt, report this vulnerability and wait for the manufacturer to comment;;

Gerando sua CVE

Gerando sua CVE

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



Common Vulnerabilities and Exposures

The de facto international standard for vulnerability identification and naming

Submit a CVE Request

* Required

* **Select a request type** - Please choose an action -

* **Enter your e-mail address** Please enter a valid e-mail address where we can reach you.

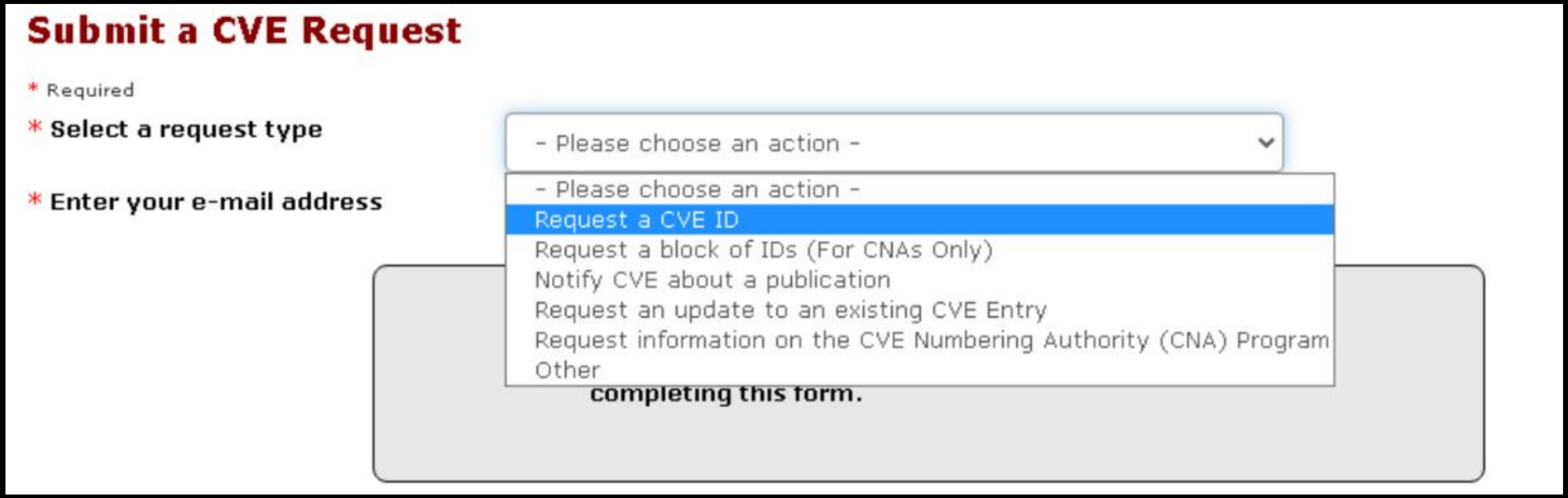
IMPORTANT: Please add cve-request@mitre.org and cve@mitre.org as safe senders in your email client before completing this form.

Enter a PGP Key (to encrypt)

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.

Gerando sua CVE

- Clique em Select a Request Type: Request a CVE ID



Submit a CVE Request

* Required

* **Select a request type** - Please choose an action -

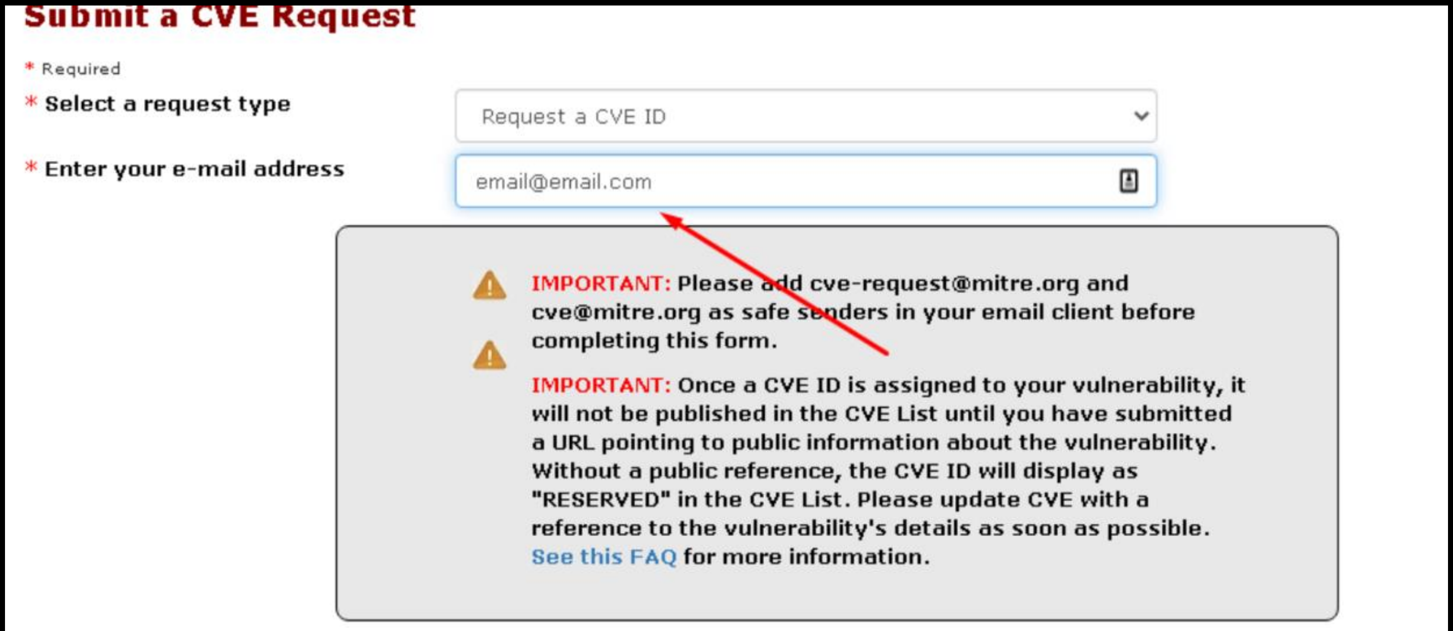
* **Enter your e-mail address**

completing this form.

- 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

Gerando sua CVE

- Digite o seu endereço de e-mail



Submit a CVE Request

* Required

* Select a request type: Request a CVE ID

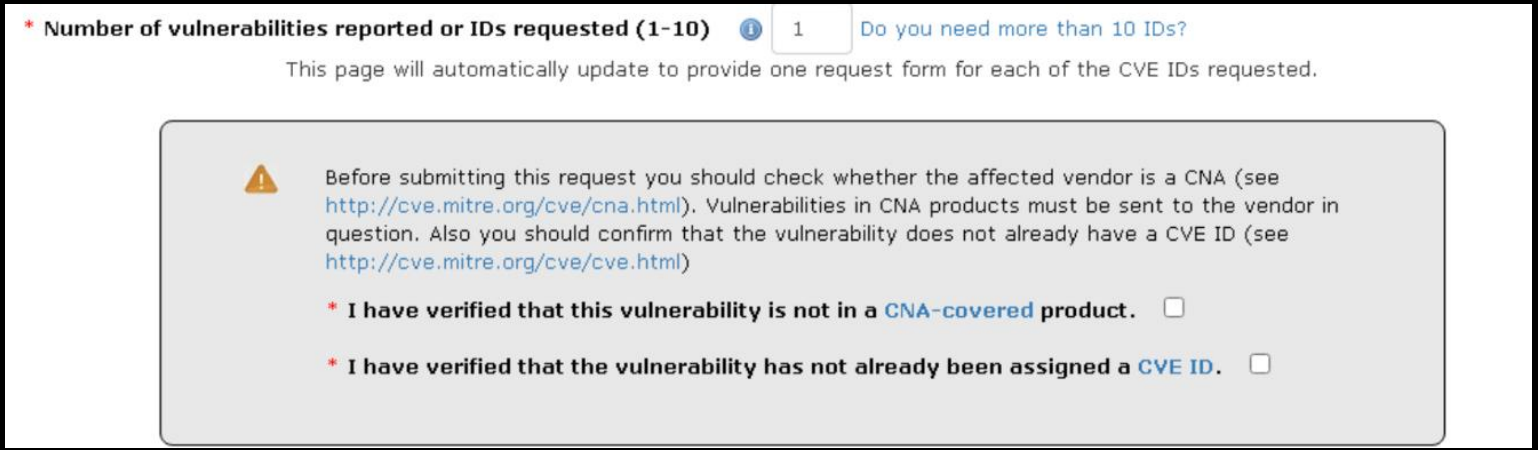
* Enter your e-mail address: email@email.com

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.

Gerando sua CVE

- Você pode definir o número de IDs de CVE. Caso for reportar múltiplas vulnerabilidades, permitindo até 10 por requisição



* **Number of vulnerabilities reported or IDs requested (1-10)** 1 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)

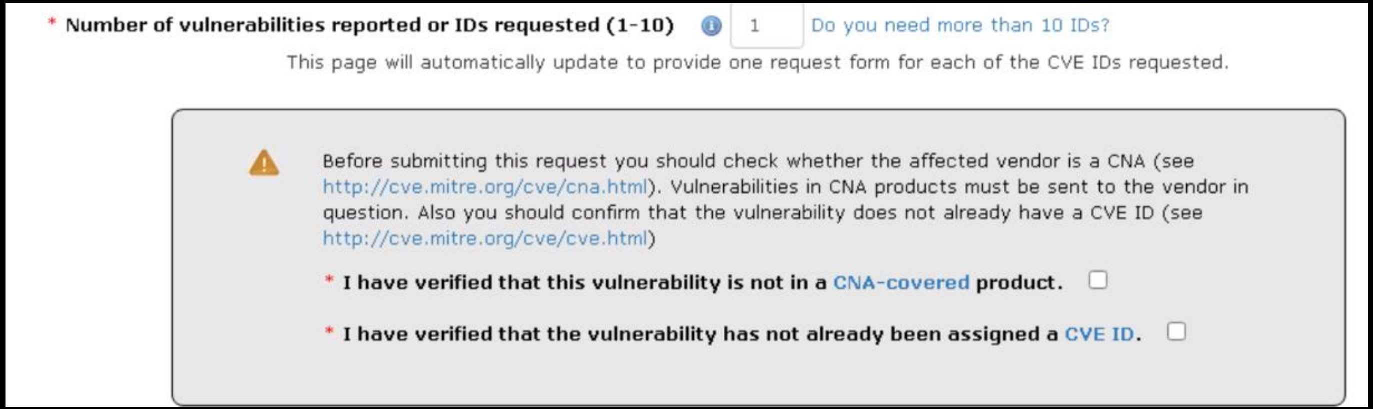
* **I have verified that this vulnerability is not in a CNA-covered product.** □

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

Gerando sua CVE

- As CNAs são os responsáveis pela atribuição dos IDS da CVE e por manter essas informações, além de 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;



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

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

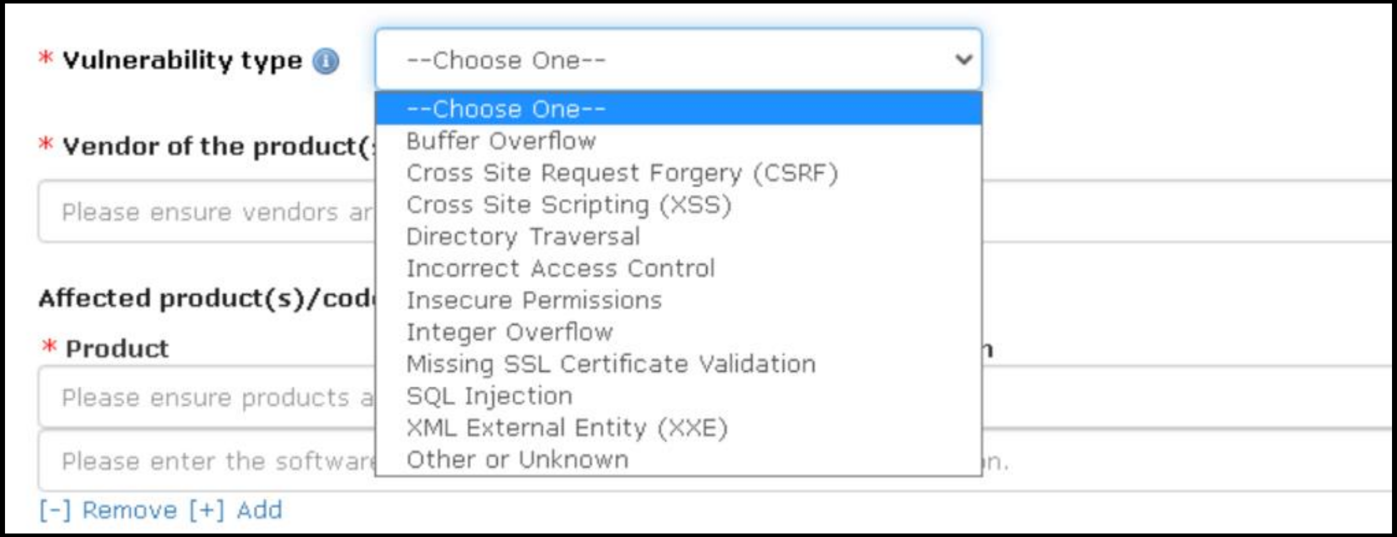
⚠ Before submitting this request you should check whether the affected vendor is a CNA (see http://cve.mitre.org/cve/cna.html). Vulnerabilities in CNA products must be sent to the vendor in question. Also you should confirm that the vulnerability does not already have a CVE ID (see http://cve.mitre.org/cve/cve.html)

* **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.** □

Gerando sua CVE

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



* **Vulnerability type** --Choose One--

- --Choose One--
- 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)
- Other or Unknown

* **Vendor of the product(**

Please ensure vendors ar

Affected product(s)/cod

* **Product**

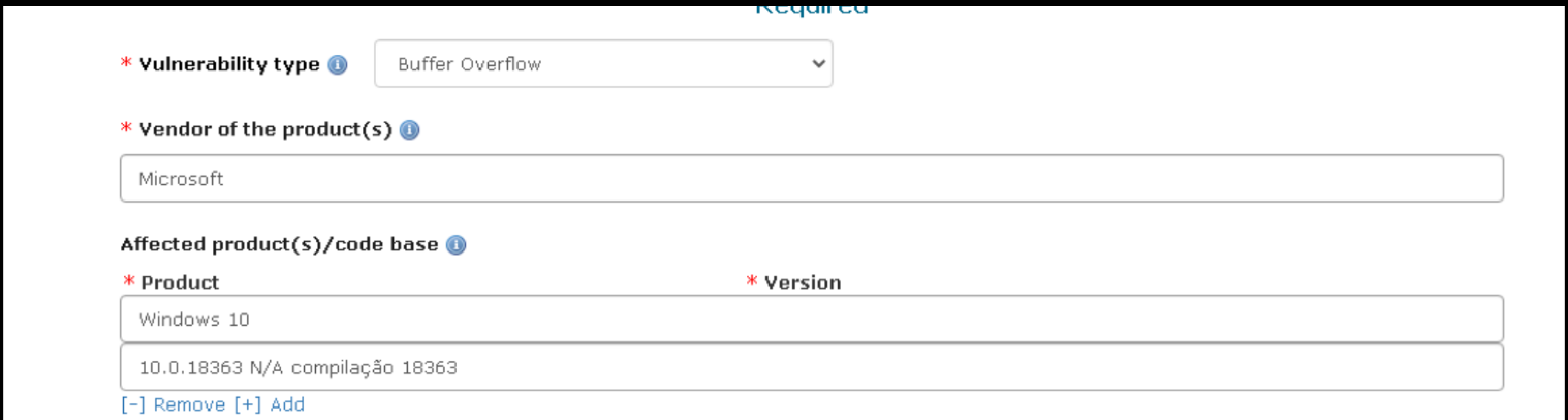
Please ensure products a

Please enter the softwar

[-] Remove [+] Add

Gerando sua CVE

- Adicione o nome do Fabricante do produto, nome do produto afetado e sua versão.
- *Exemplo abaixo: Nome da fabricante é Microsoft, nome do produto Windows 10 e a versão da Build 10.0.18363*



* **Vulnerability type** Buffer Overflow

* **Vendor of the product(s)**

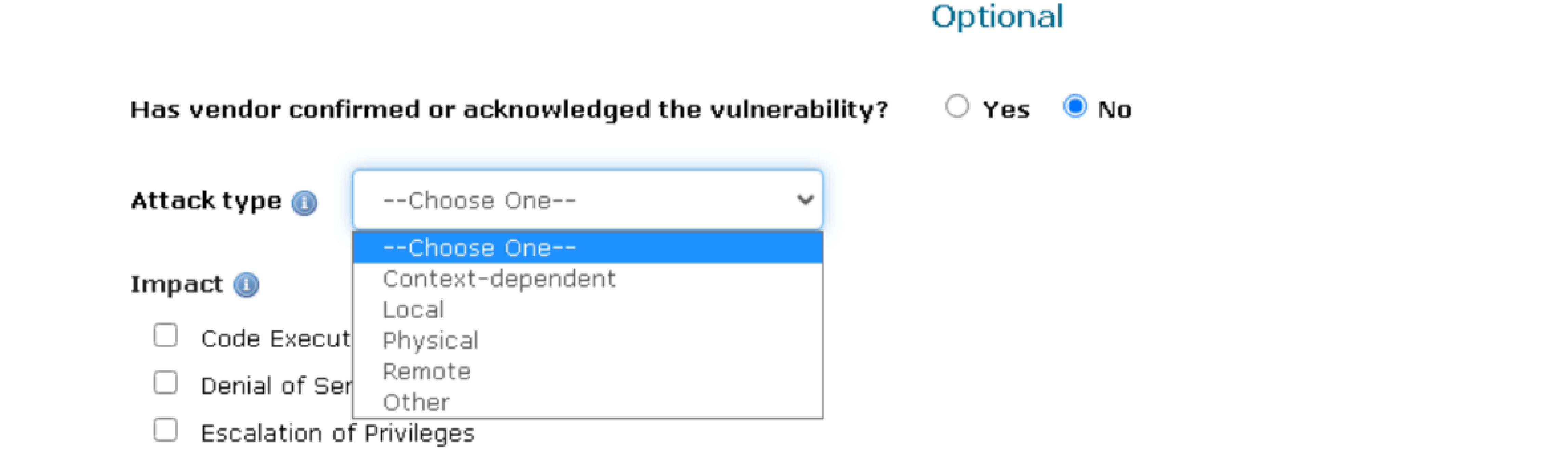
Microsoft

Affected product(s)/code base

* Product	* Version
Windows 10	
10.0.18363 N/A compilação 18363	

Gerando sua CVE

- Caso o fabricante tenha reconhecido a existência da vulnerabilidade, selecione a opção “Yes”, isso se você reportou a vulnerabilidade pro fabricante;
- E escolha o tipo de ataque, no caso, como ele é feito



Optional

Has vendor confirmed or acknowledged the vulnerability? ○ Yes ● No

Attack type: --Choose One--

Impact

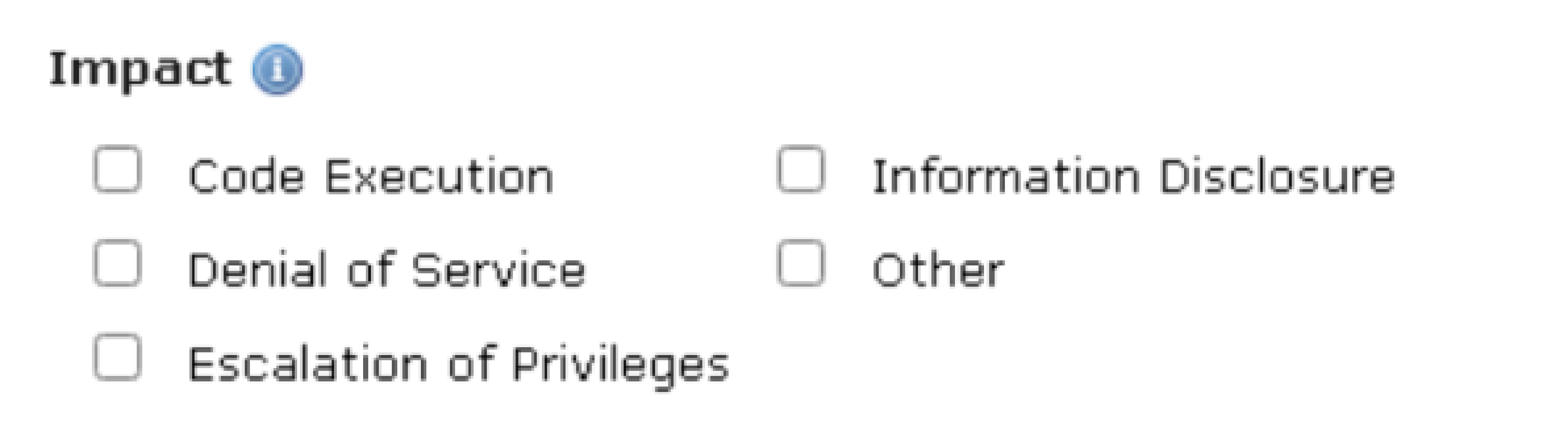
□ Code Execut

□ Denial of Ser

□ Escalation of Privileges

Gerando sua CVE

- Selecione o impacto que a vulnerabilidade pode trazer, caso não seja nenhuma das 4 primeiras opções, selecione “Other”

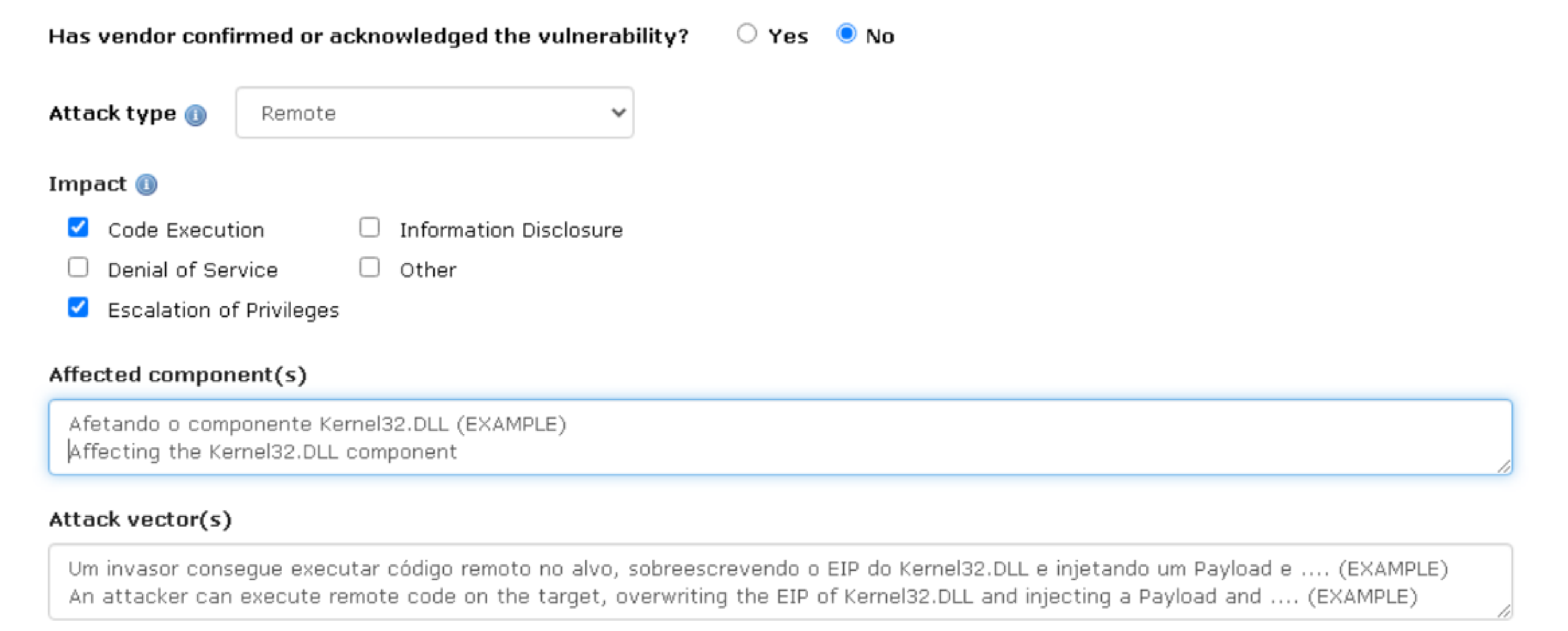


Impact ⓘ

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

Gerando sua CVE

- Um breve rascunho de exemplo. Aonde o componente afetado é geralmente uma Lib, API, função, plugin ou aquele que inicia o vetor de ataque;
- Abaixo você vai dar uma descrição de como o atacante explora a vulnerabilidade, mostrando o que é afetado no componente vulnerável;



Has vendor confirmed or acknowledged the vulnerability? ○ Yes ● No

Attack type Remote

Impact

☑ Code Execution
☐ Information Disclosure
☐ Denial of Service
☐ Other
☑ Escalation of Privileges

Affected component(s)

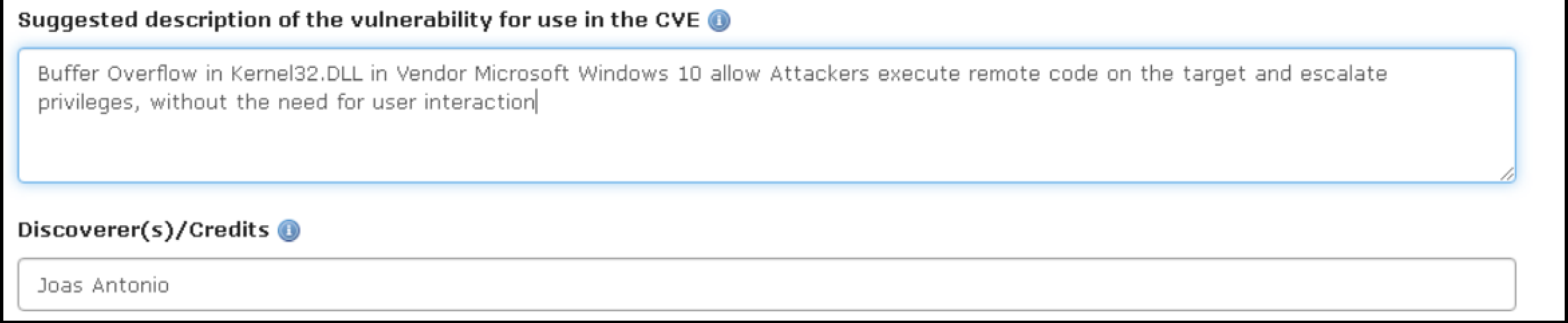
Afetando o componente Kernel32.DLL (EXAMPLE)
Affecting the Kernel32.DLL component

Attack vector(s)

Um invasor consegue executar código remoto no alvo, sobreescrevendo 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)

Gerando sua CVE

- Abaixo você tem um exemplo de descrição que vai aparecer para todos quando sua CVE for gerada;
- Uma descrição da vulnerabilidade não precisa conter o exploit, só resumir o que se trata a vulnerabilidade e qual componente é afetado, a versão do produto e seu tipo.
- *Lembre-se que a Prova do Conceito é importante, quando sair a correção você pode postar em seu blog ou redes sociais, pois assim a sua 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

CVE Reserved

- Hoje muitas CVEs ficam em um estado de Reservado, isso se dá pois a vulnerabilidade entra em um processo de discussão, dependendo do seu grau de importância ela tem sua descrição revelada, mas se não, você vai ter que aguardar por um tempo. Geralmente quando se reporta para um CNA, eles já possuem CVE IDs prontos para serem alocados, caso ao contrário o processo se torna demorado.

A comunicações que ocorre entre os CNAs para o MITRE são as seguintes:

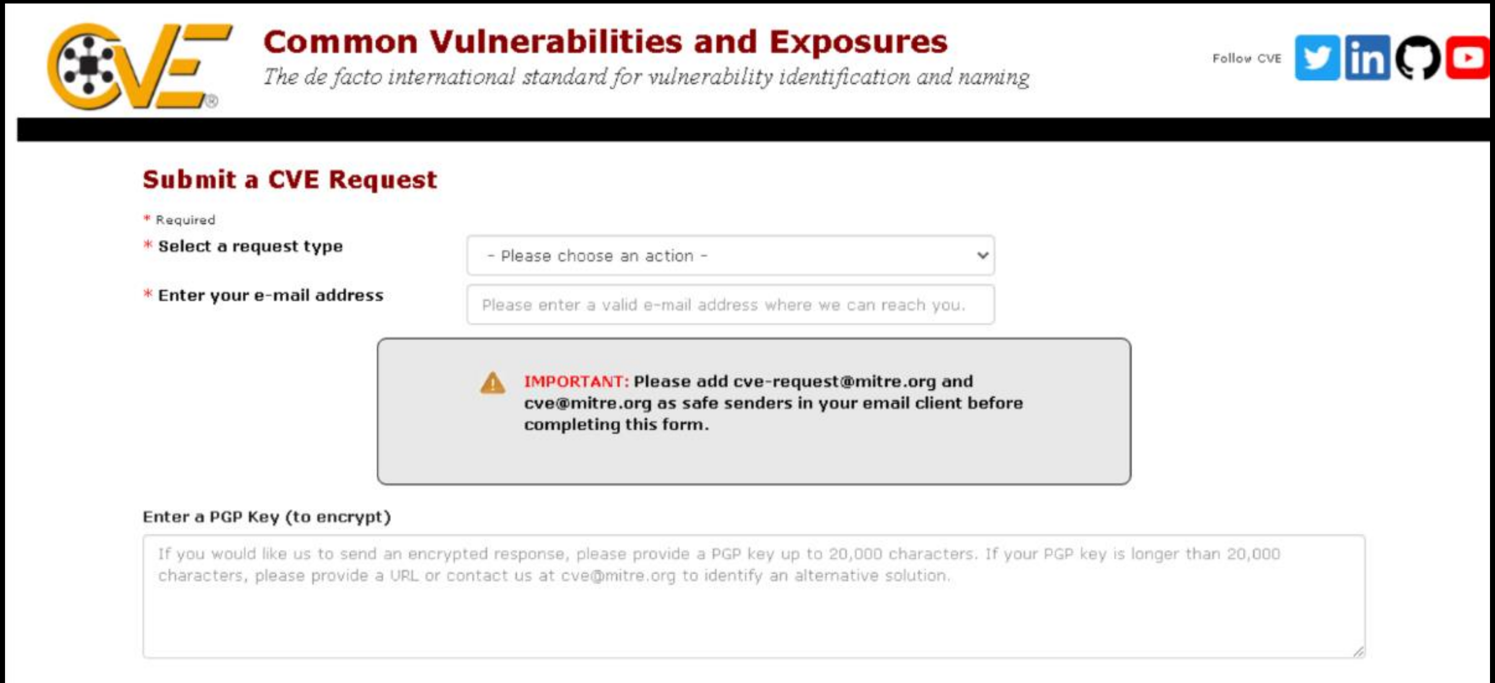
- (1) O CNA solicita um pool de IDs de CVE.
- (2) A CNA anuncia a publicação de um novo CVE ID, que permite ao MITRE atualizar as informações do CVE ID no site do CVE.
- (3) O CNA pode precisar consultar o MITRE sobre as decisões de conteúdo do CVE.
- (4) A CNA notifica o MITRE sobre suspeitas de abusos do processo CVE por pesquisadores.
- (5) O CNA notifica o MITRE e outras partes quando são detectados IDs CVE duplicados.

cve.mitre.org

Generating your CVE

Generating your CVE

- Visit the website: https://cveform.mitre.org



Common Vulnerabilities and Exposures

The de facto international standard for vulnerability identification and naming

Submit a CVE Request

* Required

* **Select a request type** - Please choose an action -

* **Enter your e-mail address** Please enter a valid e-mail address where we can reach you.

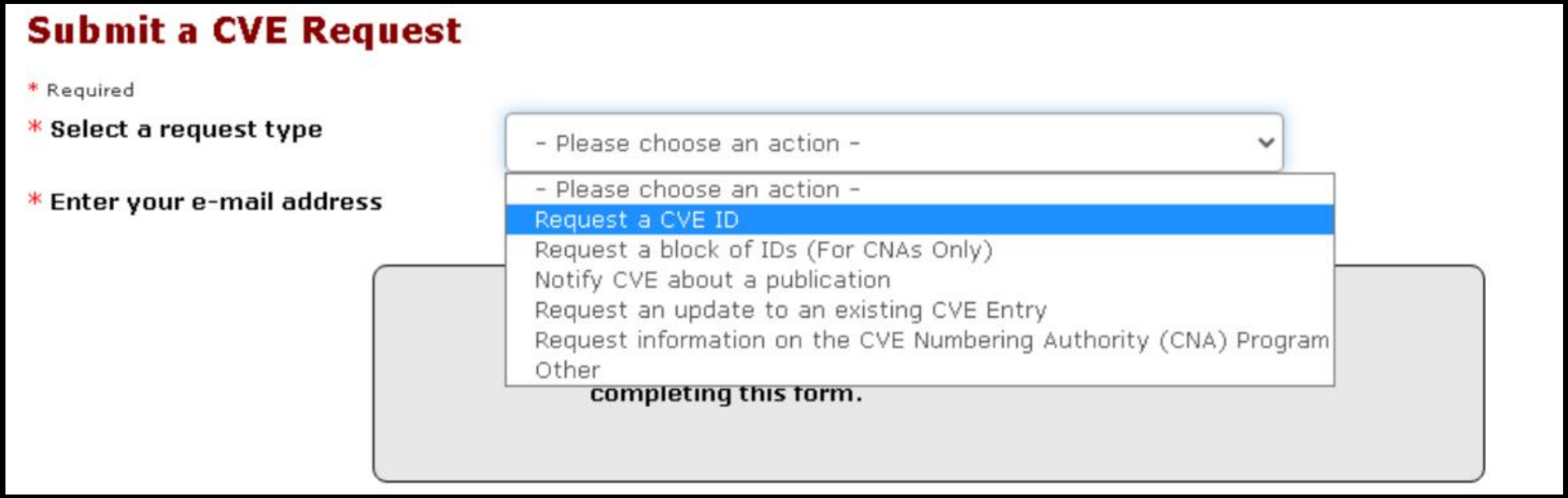
IMPORTANT: Please add cve-request@mitre.org and cve@mitre.org as safe senders in your email client before completing this form.

Enter a PGP Key (to encrypt)

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.

Generating your CVE

- Clique em Select a Request Type: Request a CVE ID



Submit a CVE Request

* Required

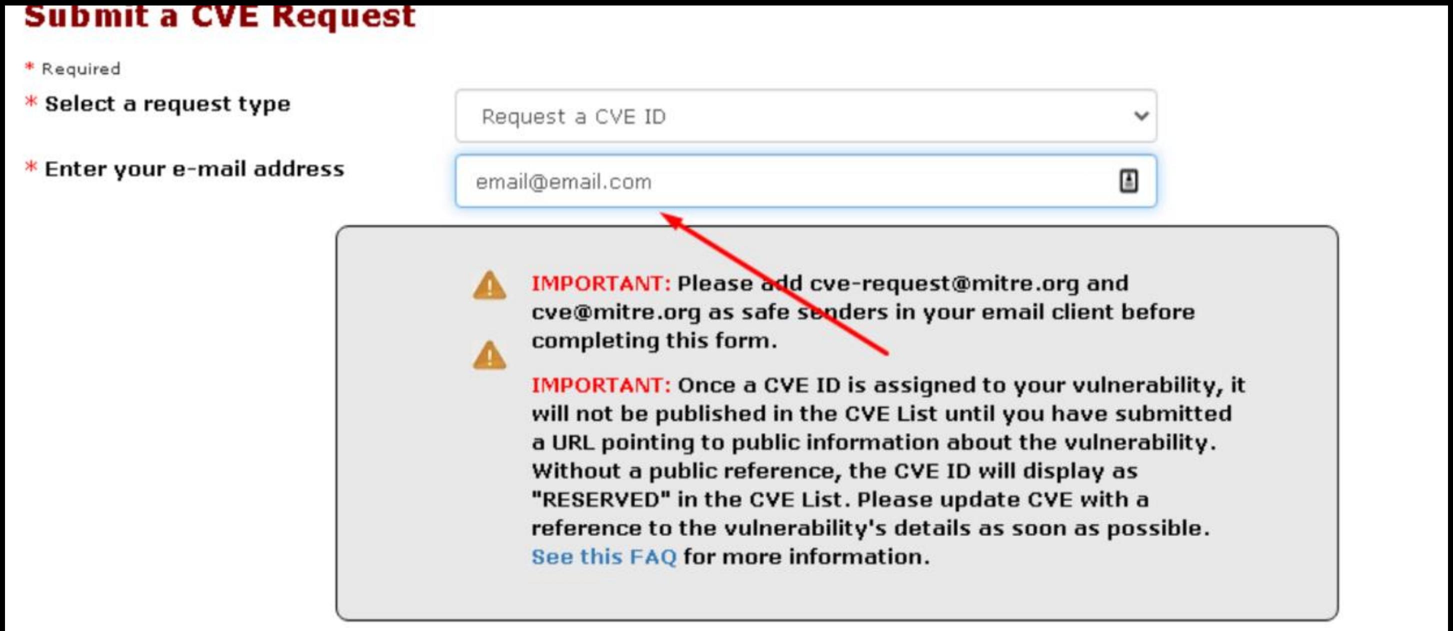
* **Select a request type** - Please choose an action -

* **Enter your e-mail address**

- 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.

Generating your CVE

- Digite o seu endereço de e-mail



Submit a CVE Request

* Required

* **Select a request type** Request a CVE ID

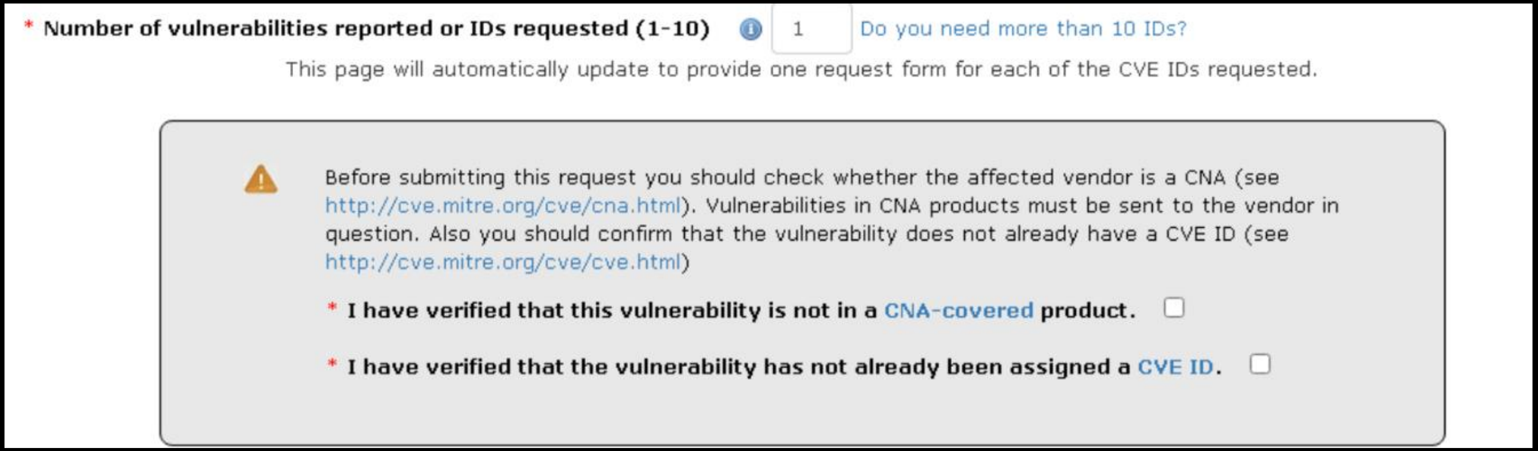
* **Enter your e-mail address** email@email.com

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.

Generating your CVE

- Você pode definir o número de IDs de CVE. Caso for reportar múltiplas vulnerabilidades, permitindo até 10 por requisição



* Number of vulnerabilities reported or IDs requested (1-10) 1 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)

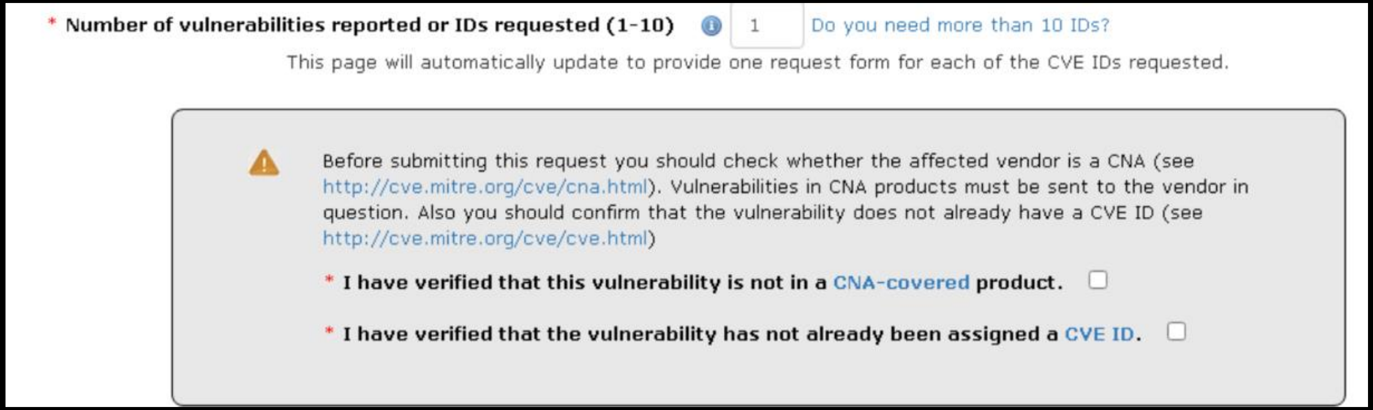
* I have verified that this vulnerability is not in a CNA-covered product. □

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

Generating your CVE

- As CNAs são os responsáveis pela atribuição dos IDS da CVE e por manter essas informações, além de 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;



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

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

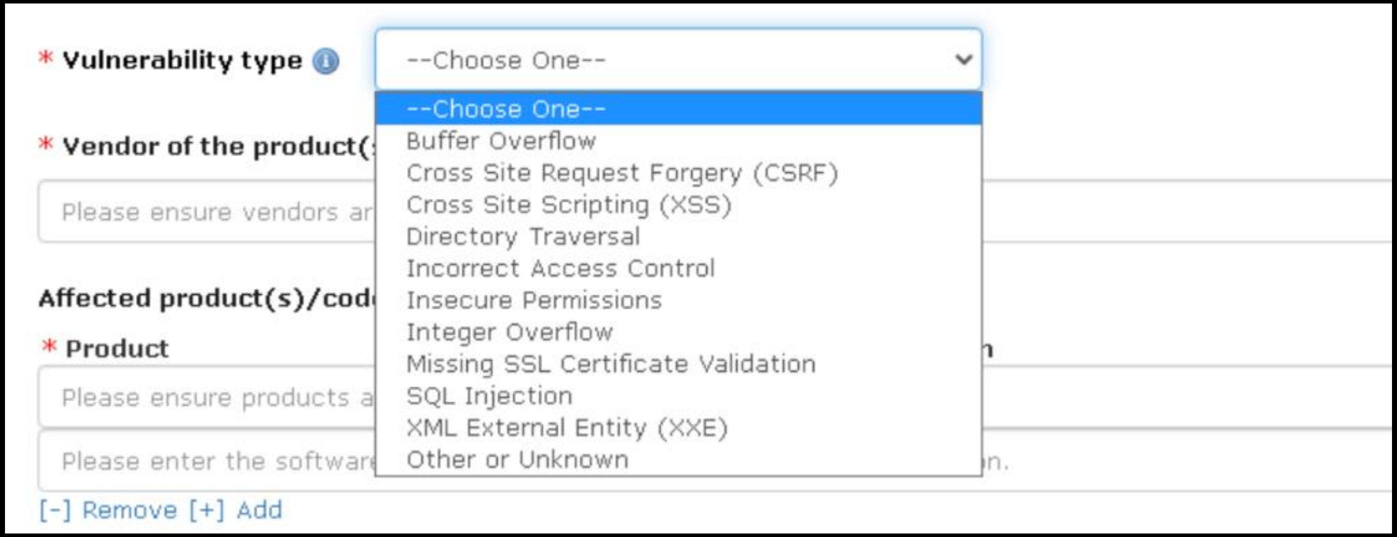
Before submitting this request you should check whether the affected vendor is a CNA (see http://cve.mitre.org/cve/cna.html). Vulnerabilities in CNA products must be sent to the vendor in question. Also you should confirm that the vulnerability does not already have a CVE ID (see http://cve.mitre.org/cve/cve.html)

* **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.** □

Generating your CVE

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



* **Vulnerability type** --Choose One--

--Choose One--
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)
Other or Unknown

* **Vendor of the product(**

Please ensure vendors ar

Affected product(s)/cod

* **Product**

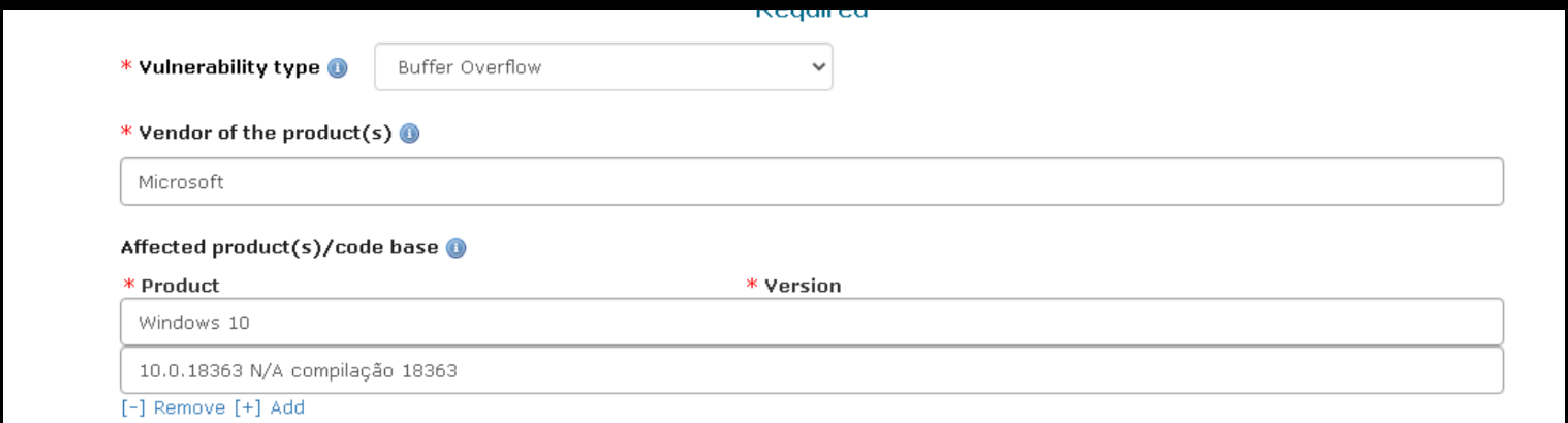
Please ensure products a

Please enter the softwar

[-] Remove [+] Add

Generating your CVE

- Adicione o nome do Fabricante do produto, nome do produto afetado e sua versão.
- *Exemplo abaixo: Nome da fabricante é Microsoft, nome do produto Windows 10 e a versão da Build 10.0.18363*



Required

* Vulnerability type: Buffer Overflow

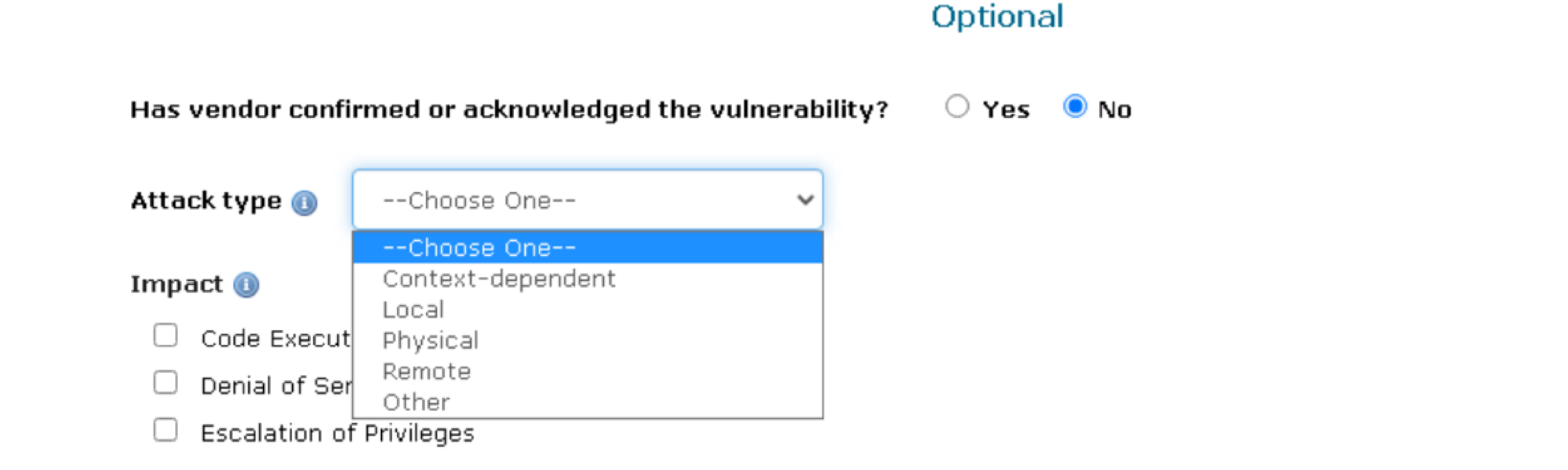
* Vendor of the product(s): Microsoft

Affected product(s)/code base

* Product	* Version
Windows 10	
10.0.18363 N/A compilação 18363	

Generating your CVE

- If the manufacturer has recognized the existence of the vulnerability, select the “Yes” option, if you have reported the vulnerability to the manufacturer;
- And choose the type of attack, in the case, how it is done



Optional

Has vendor confirmed or acknowledged the vulnerability? ○ Yes ● No

Attack type: --Choose One--

Impact

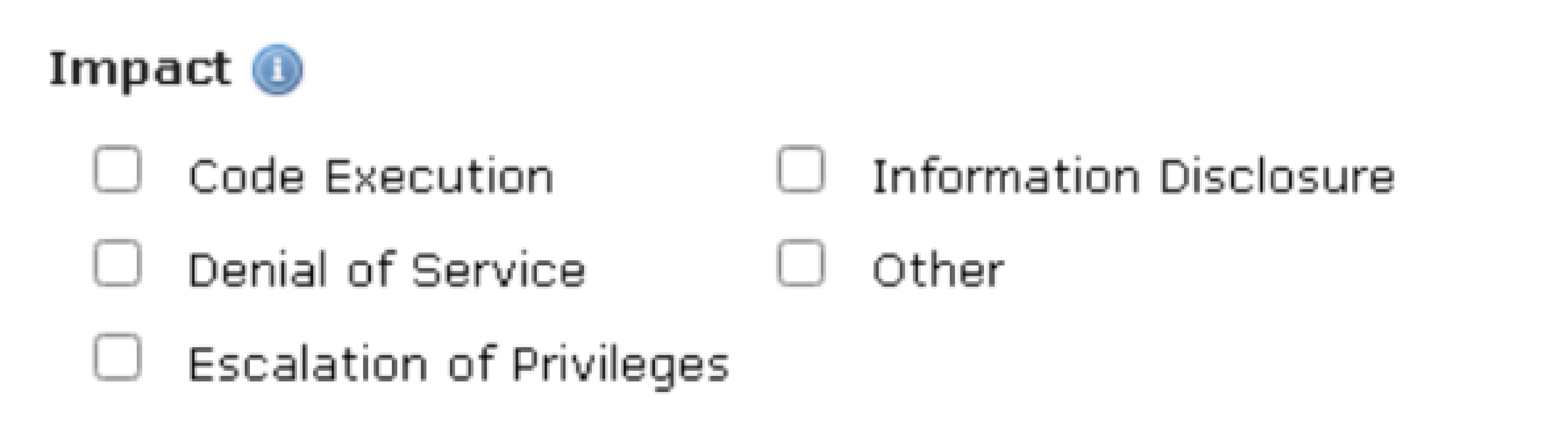
□ Code Execut

□ Denial of Ser

□ Escalation of Privileges

Generating your CVE

- Select the impact that the vulnerability can bring, if it is not one of the first 4 options, select “Other”



Impact

□ Code Execution

□ Denial of Service

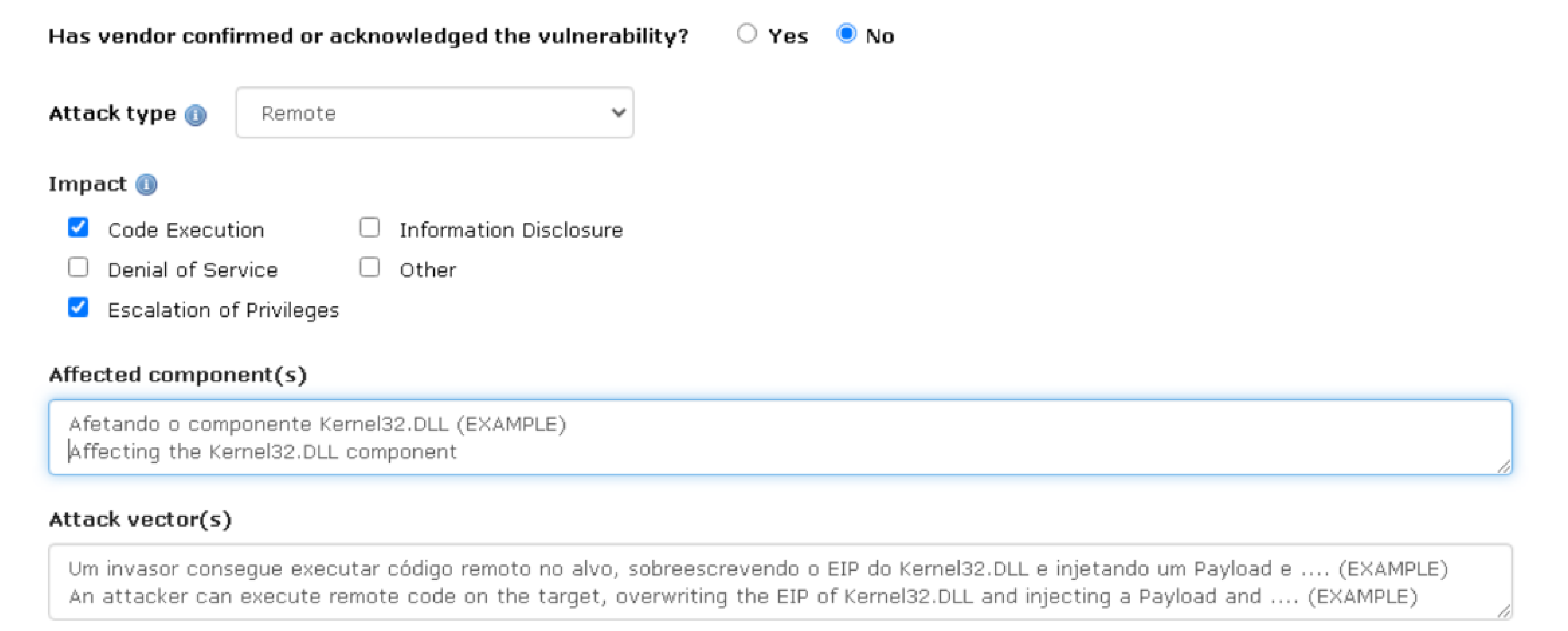
□ Escalation of Privileges

□ Information Disclosure

□ Other

Generating your CVE

- A brief example sketch. Where the affected component is usually a Lib, API, function, plugin or the one that initiates the attack vector;
- Below you will give a description of how the attacker exploits the vulnerability, showing what is affected in the vulnerable component;



Has vendor confirmed or acknowledged the vulnerability? ○ Yes ● No

Attack type: Remote

Impact

☑ Code Execution ☐ Information Disclosure

☐ Denial of Service ☐ Other

☑ Escalation of Privileges

Affected component(s)

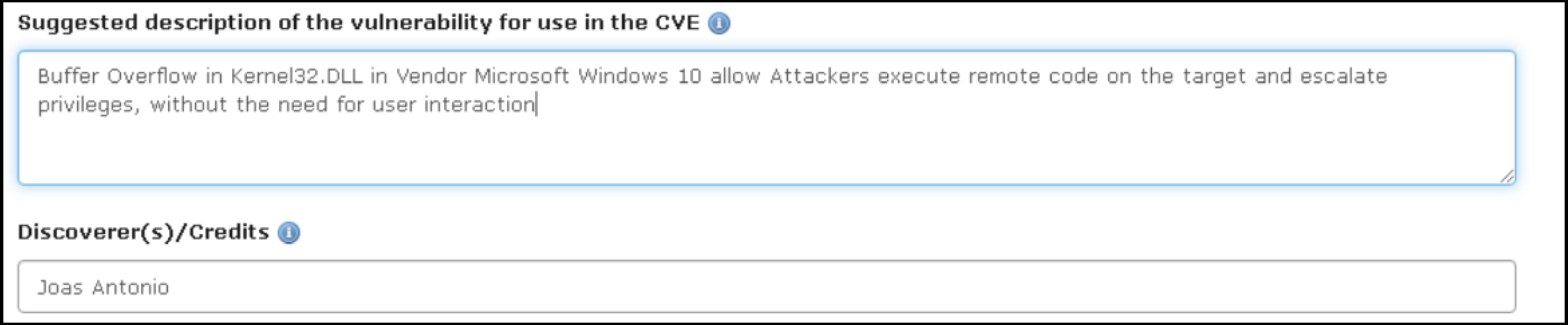
Afetando o componente Kernel32.DLL (EXAMPLE)
Affecting the Kernel32.DLL component

Attack vector(s)

Um invasor consegue executar código remoto no alvo, sobreescrevendo 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)

Generating your CVE

- Below you have an example description that will appear for everyone when your CVE is generated;
- A vulnerability description does not need to contain the exploit, it only summarizes what the vulnerability is and which component is affected, the product version and its type.
- Remember that the Proof of Concept is important, when the fix comes out you can post it on your blog or social networks, so your CVE becomes an Identifier to help other companies fix such identified vulnerability.



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

CVE Reserved

- Today many CVEs are in a Reserved state, this is because the vulnerability enters a discussion process, depending on its degree of importance it has its description revealed, but if not, you will have to wait for a while. Usually when reporting to a CNA they already have CVE IDs ready to be allocated, otherwise the process becomes time consuming.

The communications that take place between the CNAs for MITER are as follows:

- (1) CNA requests a pool of CVE IDs.
- (2) CNA announces the publication of a new CVE ID, which allows MITER to update CVE ID information on the CVE website.
- (3) The CNA may need to consult with MITER regarding CVE content decisions.
- (4) CNA notifies MITER of suspected abuses of the CVE process by researchers.
- (5) CNA notifies MITER and other parties when duplicate CVE IDs are detected.