

You have **2** free member-only stories left this month. [Sign up for Medium and get an extra one](#)

How to register and publish a CVE for your awesome vulnerability



Raimonds Liepins [Follow](#)

Jan 28 · 3 min read ★



Source: cve.mitre.org

Common vulnerabilities and exposures allow the security community to see issues associated with the current product version and see if they need to upgrade as well as provide context like with “CVE-2020-25268” which is a RCE vulnerability on Ilias Learning Management System. If you would search for that you would see a link here “<https://nvd.nist.gov/vuln/detail/CVE-2020-25268>” that leads to a bunch of useful information regarding CVSS score, advisories, POC’s, descriptions etc.

CVSS 3.x Severity and Metrics:



NIST: NVD

Base Score: 8.8 HIGH

Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.


References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have

information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
https://medium.com/bugbountywriteup/exploiting-ilias-learning-management-system-4eda9e120620	Exploit Third Party Advisory

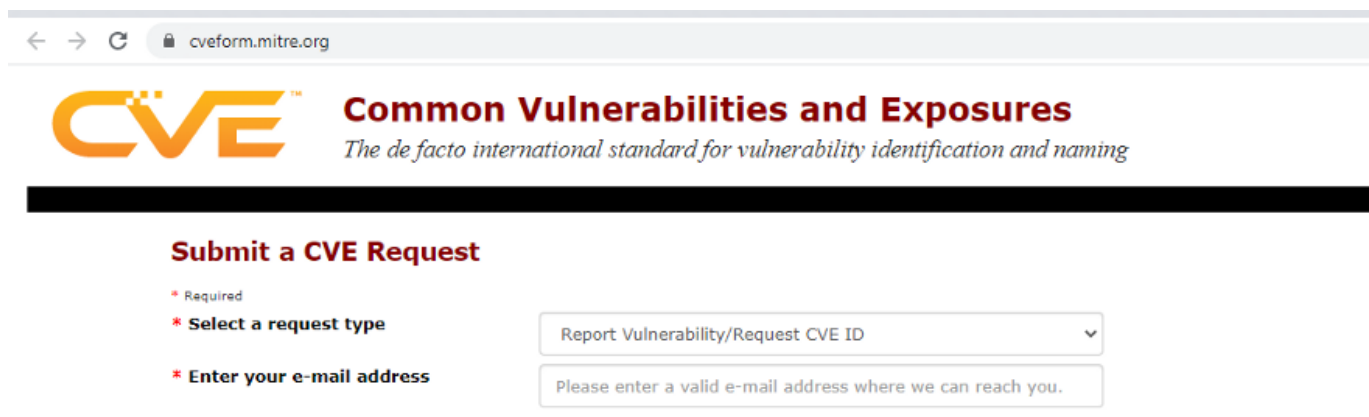
Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-74	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	 NIST

I hope we can all agree that CVE's are cool to have, however not all CVE's are created equal. As well as the CVSS score describing the severity of CVE can sometimes be rather useless, since multiple low scored vulnerabilities might be chained together creating a critical 10/10 and there's no way to showcase that in the current model.

How do you actually register one?

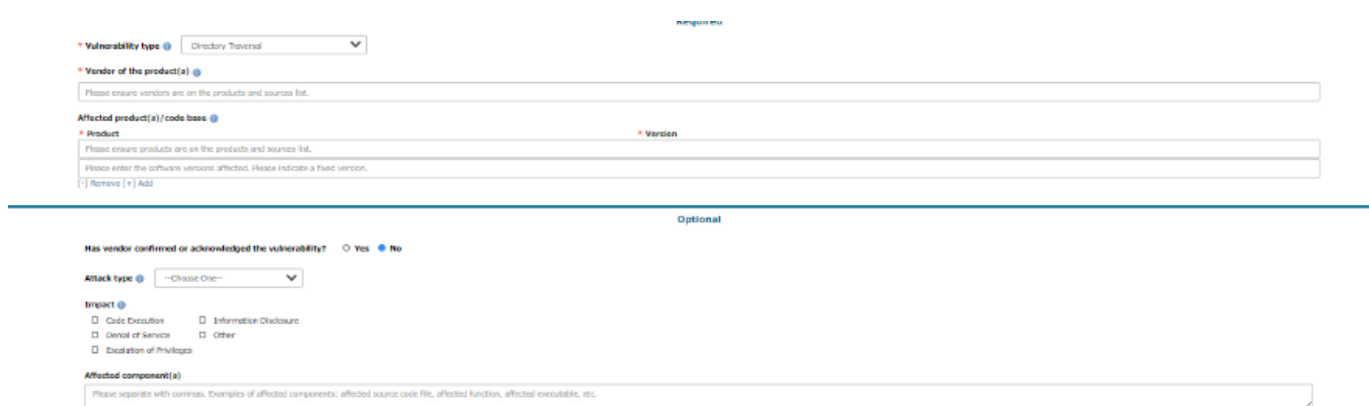
You just go to <https://cveform.mitre.org> and register your CVE and that's it or is it?



The screenshot shows the CVE Form registration page. At the top, there's a navigation bar with the CVE logo and the text "Common Vulnerabilities and Exposures" and "The de facto international standard for vulnerability identification and naming". Below this is a section titled "Submit a CVE Request". It contains three required fields: "Select a request type" (a dropdown menu with "Report Vulnerability/Request CVE ID" selected), "Enter your e-mail address" (a text input field with a placeholder "Please enter a valid e-mail address where we can reach you."), and "Vendor of the product(s)" (a text input field with a placeholder "Please ensure vendors are on the products and sources list."). There are also optional fields for "Affected product(s)/code base" and "Version".

Source: cveform.mitre.org

Well, not really. First of all there's a bunch of stuff you need to fill out.



The screenshot shows the CVE Form registration page with the optional fields expanded. It includes a section titled "Optional" with the following fields: "Has vendor confirmed or acknowledged the vulnerability?" (radio buttons for Yes and No), "Attack type" (a dropdown menu with "Choose One" selected), "Impact" (checkboxes for Code Execution, Denial of Service, Escalation of Privileges, Information Disclosure, and Other), and "Affected component(s)" (a text input field with a placeholder "Please separate with commas. Examples of affected components: affected source code file, affected function, affected executable, etc.").

[Cve](#) [Security](#) [Penetration Testing](#)

[About](#) [Help](#) [Legal](#)

Get the Medium app



Attack vector(s)
What are the methods of exploitation? Example: to exploit vulnerability, someone must open a crafted JPEG file.
Suggested description of the vulnerability for use in the CVE
Discoverer(s)/Credits
Individual(s) or organization(s) that found the vulnerability or reported the vulnerability to you.
Reference(s)
Please include one reference/URL per line including protocol and domain name, e.g., www.blink.com https://link.org
Additional information
Please provide any additional information you want to share with us here.

To help you with this here's a really great material on that.

[“http://cveproject.github.io/docs/content/key-details-phrasing.pdf”](http://cveproject.github.io/docs/content/key-details-phrasing.pdf)

- If you **underreport** key details, you may not be able to make the appropriate match later on.
- If you **overreport** details, you can obscure the distinguishing details and are more prone to introduce errors.

Generic Templates

- [VULNTYPE] in [COMPONENT] in [VENDOR] [PRODUCT] [VERSION] allows [ATTACKER] to [IMPACT] via [VECTOR].
- [COMPONENT] in [VENDOR] [PRODUCT] [VERSION] [ROOT CAUSE], which allows [ATTACKER] to [IMPACT] via [VECTOR].

Default Detail Phrasing

- The following is what to do if you do not have information about a key detail.
- Vulnerability Type: Skip if applicable
 - At this level you should never encounter a vulnerability where you need to skip the type phrasing.
- Component: Skip
- Vendor: Skip
- Product: You MUST have a product name.
- Version: Skip
- Attacker: Use “attackers”
- Impact: Use “unspecified impact”

- Vectors: Use “via unspecified vectors”

Product

- [VULNTYPE] in [COMPONENT] in **IVENDOR**
[PRODUCT] [VERSION] al Page 3 / 20
[IMPACT] via [VECTOR].

Essentially it gives you templates for everything that you need in writing the CVE.

After you are done with the web form, you will receive a confirmation that the CVE is registered and you will get your number like CVE-YEAR-NUMBER (CVE-2020-25268). The issue itself won't be published until you send them a publication for the vulnerability, so until that you can communicate with the vendor to get the issue addressed. The publication can be done by the vendor if the response is present within a timeframe you have chosen and if not, you can do a publication on your own.

Important

I would strongly advise against publishing on your own without first trying multiple times establishing a contact with the vendor and making sure that vendor actually understands the vulnerability. This is critical, the CVE's are meant to help improve security not diminish it.

Best of luck registering and publishing your CVE's!

Sign up for Infosec Writeups

By InfoSec Write-ups

Newsletter from Infosec Writeups [Take a look](#)

Your email

Get this newsletter

By signing up, you will create a Medium account if you don't already have one. Review our [Privacy Policy](#) for more information about our privacy practices.