How to register and publish a CVE for your awesome vulnerability

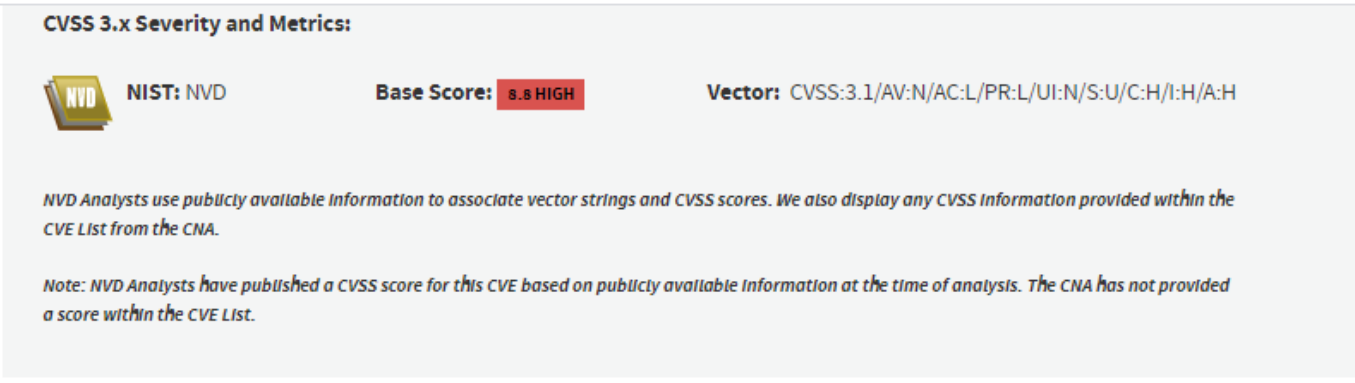
R

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.



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

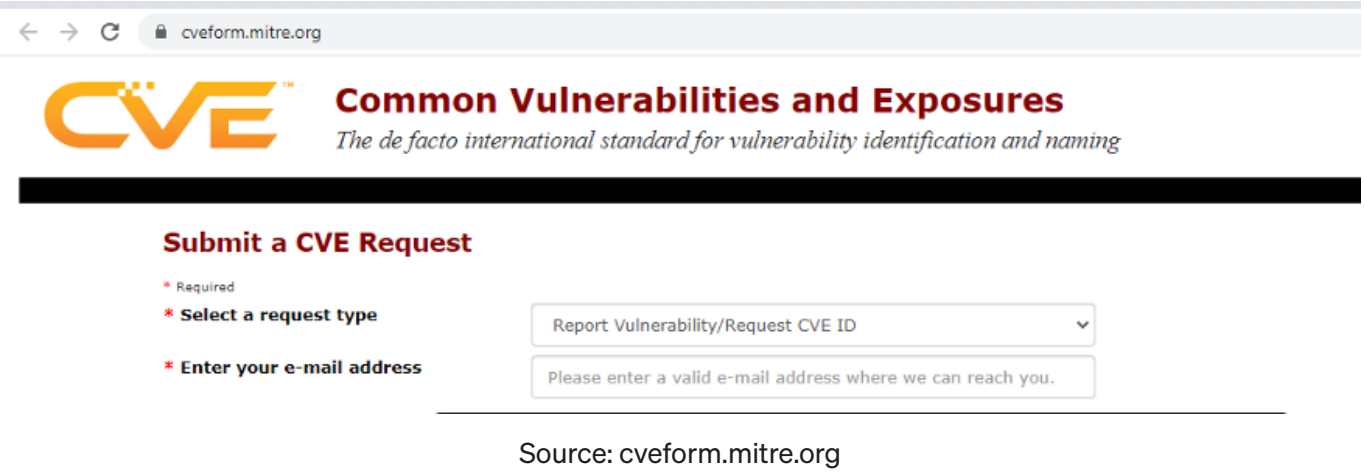
Weakness Enumeration

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.

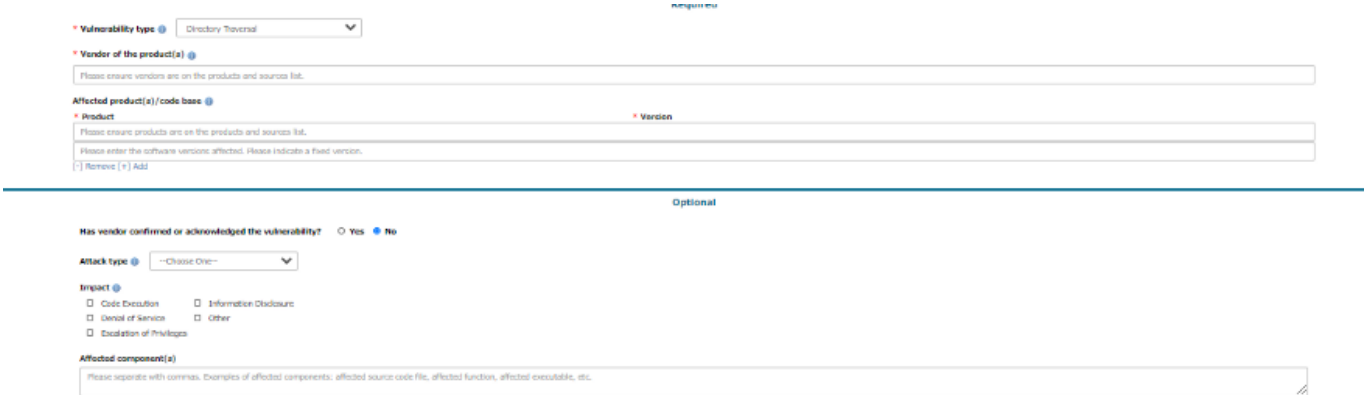
How do you actually register one?

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



Source: cveform.mitre.org

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



Cve Security Penetration Testing

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

"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.

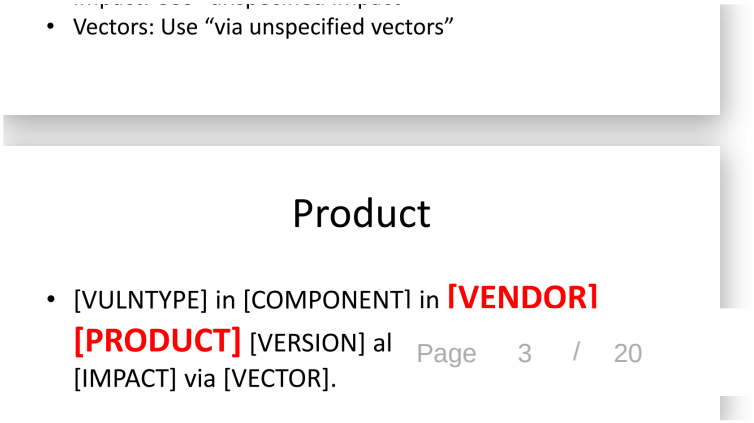
Generic Templates

- [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"



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!