

CVE in 5 Mins!

{Verneet}



Who Am I?

- Security Engineer at [Société Générale](#)
- Twitter @ [err0rrrrr](#)
- Security Blogger @ [verneet.com](#)

Agenda

- Break Myth
- Deep dive into CVE.
- How to get CVE IDs 😁
- Questions and Wrap-up

The Myth



What is CVE?

- ~~• A vulnerability mitigation~~

CVE IDs uniquely define vulnerabilities so that mitigations can be efficiently applied

- ~~• A source for vulnerability risk, impact, fix or technical info~~

Each CVE contains a unique ID, description, and references

- ~~• A tool for publicly disclosing vulnerabilities~~

CVE uses publicly disclosed vulnerability information as its source of information

CVE is Assigned by?

CVE Formatted as:

CVE-YYYY-NNNNN

YYYY = Year the vulnerability made public

NNNNN = Arbitrary digits

How to get CVE IDs?



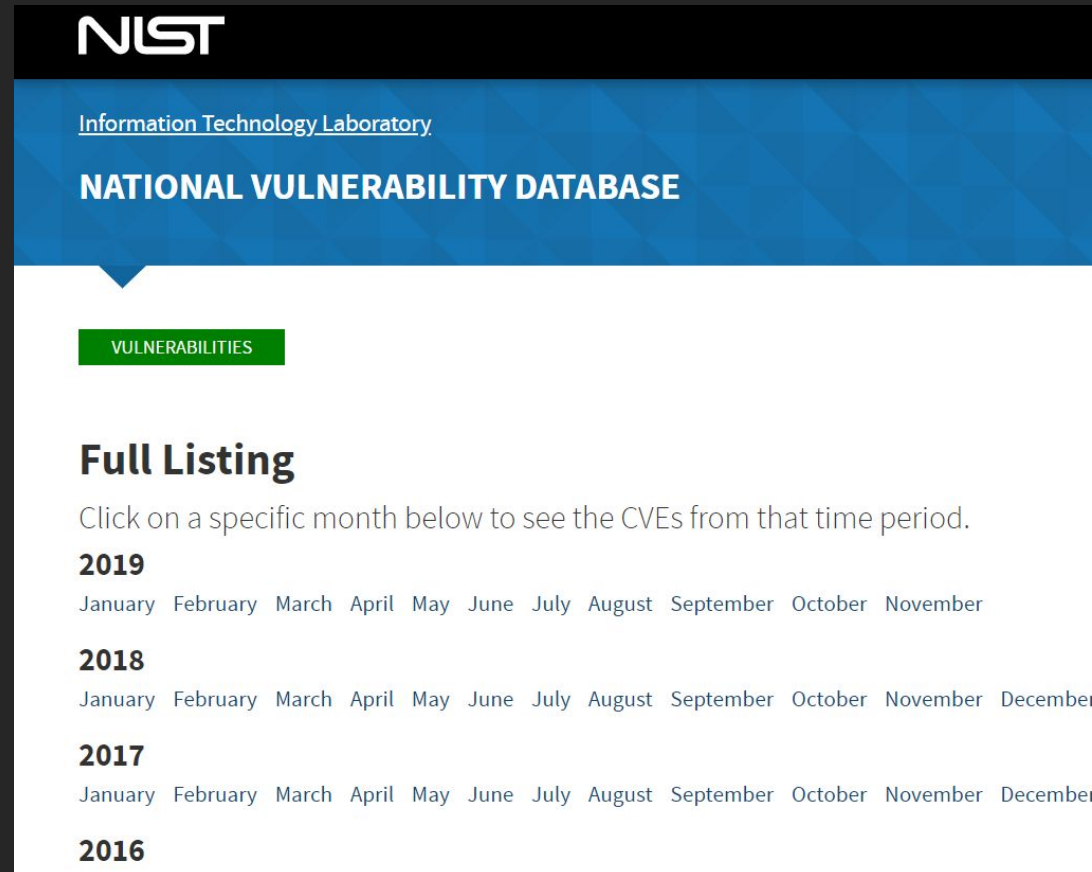
Process:

- Find the Product
- Check it's CVE listening page
- Check github
- Find a bug
- Report to vendor on there security email or github

- Apply for CVE <https://cveform.mitre.org>
- Create a public report
- Send all the Publications to MITRE
- BOOM! You got CVE under your name

Find the product:

<https://nvd.nist.gov/vuln/full-listing>



The screenshot shows the NIST National Vulnerability Database (NVD) Full Listing page. The header includes the NIST logo, the text 'Information Technology Laboratory', and 'NATIONAL VULNERABILITY DATABASE'. A green button labeled 'VULNERABILITIES' is visible. Below this, the heading 'Full Listing' is followed by the instruction 'Click on a specific month below to see the CVEs from that time period.' The page lists years from 2019 to 2016, with each year having a list of months below it.

NIST
Information Technology Laboratory
NATIONAL VULNERABILITY DATABASE

VULNERABILITIES

Full Listing

Click on a specific month below to see the CVEs from that time period.


2019
January February March April May June July August September October November

2018
January February March April May June July August September October November December


2017
January February March April May June July August September October November December

2016





<https://twitter.com/threatmeter>


 **ThreatMeter** 184.5K Tweets Follow

[Show more](#)





 **ThreatMeter** @threatmeter · 1h ⌵


Samba up to 4.9.14/4.10.9/4.11.1 Client directory traversal: A vulnerability was found in Samba up to 4.9.14/4.10... goo.gl/fb/c1oQ9U





 **ThreatMeter** @threatmeter · 1h ⌵


CVE-2006-4245 (archivemail, debian_linux): archivemail 0.6.2 uses temporary files insecurely leading to a possible... goo.gl/fb/xEQcnz





 **ThreatMeter** @threatmeter · 1h ⌵


CVE-2018-19167 (cloakcoin): CloakCoin through 2.2.2.0 (a chain-based proof-of-stake cryptocurrency) allows a... goo.gl/fb/saVH82

  1  





 **ThreatMeter** @threatmeter · 1h ⌵


Junos OS: J-Web Session Fixation Vulnerability (JSA10961): Nessus Plugin ID 130519 with Medium Severity Synopsis... goo.gl/fb/FHMJFa

 **ThreatMeter** @threatmeter · 1h ⌵

Junos OS: srpxfe DoS (JSA10972): Nessus Plugin ID 130520 with Medium Severity Synopsis The remote device is... goo.gl/fb/uMYL71

 **ThreatMeter** @threatmeter · 1h ⌵

Parallels Plesk Panel 9.5 Cross Site Scripting: Topic: Parallels Plesk Panel 9.5

Find Bug:



Report to vendor:

Description:

Environment:

Version: XX

OS: XX

Web server: XX

Database: XX

URL(s): XX

Expected and actual behavior:

Steps to reproduce the behavior:

Remediation:

Apply CVE:

<https://cveform.mitre.org>

Publish:

- # Description:
- # CVE ID:
- # Date of Disclosure:
- # Vendor, Product:
- # Severity Rating:
- # POC:
- # Credit:

<http://verneet.com/cve-2019-16686>

Publish:

Description:

CVE ID:

Date of Disclosure:

Vendor, Product:

Severity Rating:

POC:

Credit:

<http://verneet.com/cve-2019-16686/>