CVE in 5 Mins!

{Verneet}

Who Am I?

- Security Engineer at Société Générale
- Twitter @ err0rrrrrr
- 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?

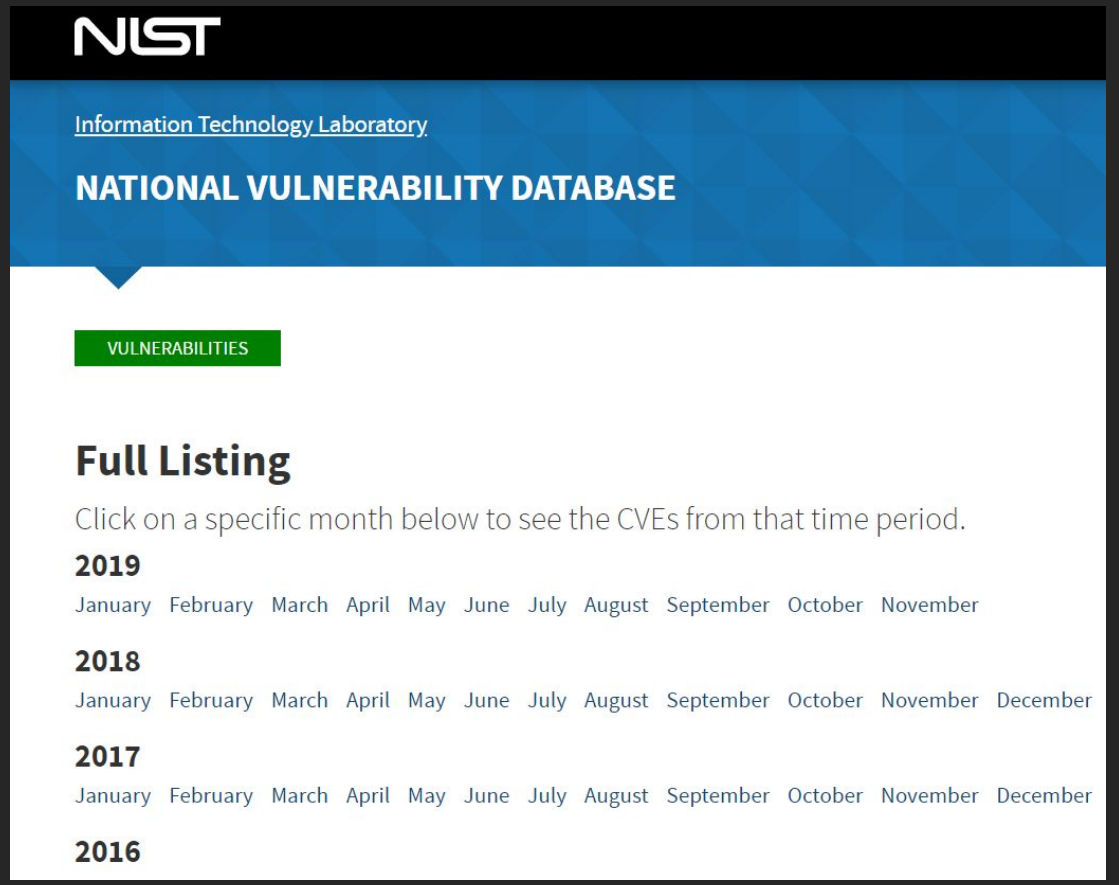
Process:

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

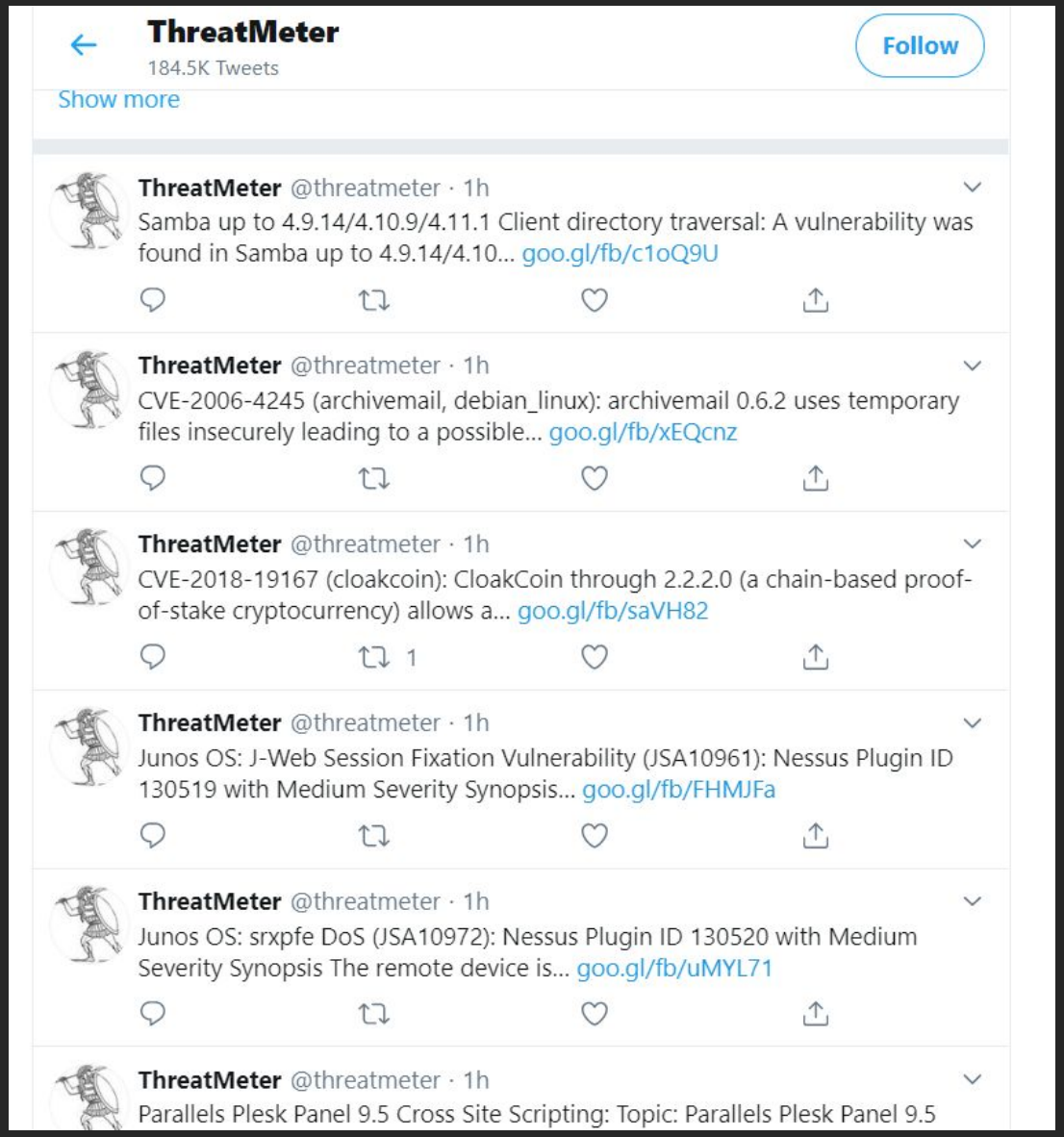
- Apply for CVE https://cveform.mitre.org
- Create a public report
- Send all the Publications to MITRE
- BOOM! You got CVE under your name

Find the product:

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



https://twitter.com/threatmeter



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/