Centro de
Investigación en
Computación

MITRE CVE

Resumen

Background

Course

Ciberseguridad

Instructor

Acosta Bermejo Raúl

Lecture notes

2025-A
Febrero del 2025
Última actualizacioón

Instituto
Politécnico
Nacional

Table of contents (outline)

Tabla de contenido

1. Introducción
2. CVE
3. Exploits
4. Herramientas

Introducción

Definiciones

Introducción

Definiciones

Bases de datos de vulnerabilidades

1. Existen varias que son gratuitas y comerciales.
2. Las grandes empresas suelen publicar las suyas, pero solo cuando ya las corrigieron.
   i. Microsoft Security Bulletin
      Por ejemplo, el código MS17-023
      https://learn.microsoft.com/en-us/security-updates/
   ii. MacOS X
      https://support.apple.com/en-us/HT201222
3. A la corrección se le llama parche, en inglés *patch*.
   i. Se utiliza un algoritmo que remplaza bytes (txt o bin) y es del tipo usado en el comando diff.

CVE

Definiciones

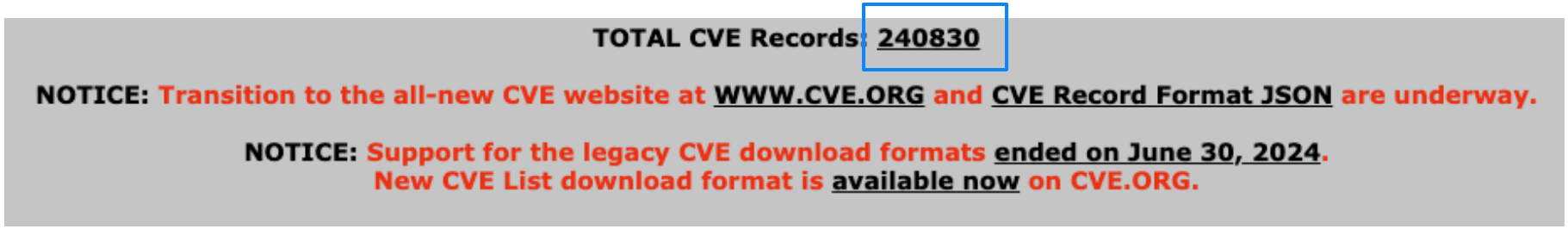
CVE

Definición

CVE (Common Vulnerabilities and Exposures)

- The mission of the CVE Program is to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities.
- URLs
  - https://cve.mitre.org/

Captura de Sitio
19 de feb de 2025



CVE

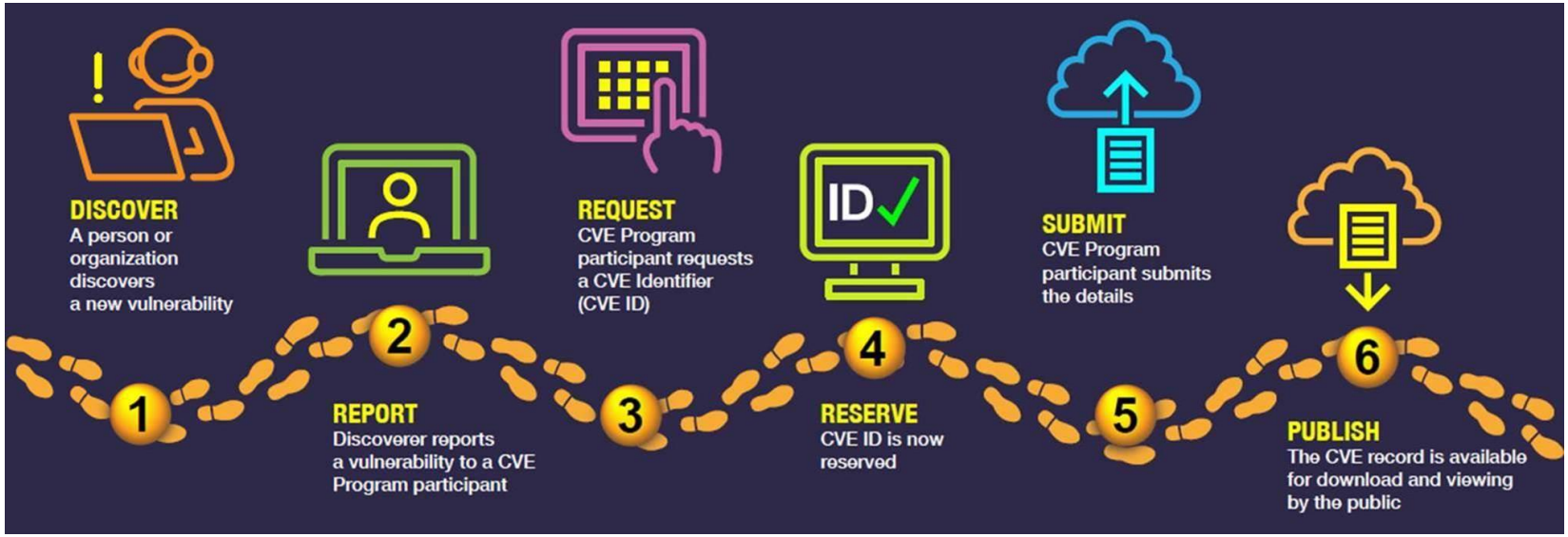
Definición

There is one CVE Record for each vulnerability on the CVE List.

Process

Vulnerabilities are:

1. First discovered, then reported to the CVE Program.
2. The reporter requests a CVE ID, which is then reserved for the reported vulnerability.
3. Once the reported vulnerability is confirmed by the identification of the minimum required data elements for a CVE Record, the record is published to the CVE List.
4. CVE Records are published by CVE Program partners from around the world.



CVE

Definición

Métricas

Published CVE Records

Comparison of published **CVE Records** by quarter

A CVE Record contains descriptive data, (i.e., a brief descr
associated with a **CVE ID**. CVE Records are published by

Year	2024	2023	2022	2021
Qtr4	11,073	7,876	6,231	5,200
Qtr3	8,591	6,936	6,448	5,541
Qtr2	11,716	7,134	6,365	5,005
Qtr1	8,697	7,015	6,015	4,415
TOTAL	40,077	28,961	25,059	20,161

CNA Partners Added by Year

Comparison of **CVE Numbering Authority (CNA)** partners

Currently, there are **442 CNAs** (440 CNAs and 2 CNA-LRs) from 4
in the CVE Program.

*Note: Occasionally, CNAs become inactive due to corporate merge
deactivated CNAs* are not removed *from the recruitment total CNA
Therefore, the totals by year columns if added together will not ma*

Year	2025	2024	2023	2022	2021
January	3	10	4	1	3
February	7	7	9	2	1
March	TBA	5	5	3	9
April	TBA	4	6	3	5
May	TBA	9	8	5	1
June	TBA	6	8	5	10
July	TBA	9	4	6	2
August	TBA	6	8	5	3
September	TBA	8	8	1	8
October	TBA	7	9	12	9
November	TBA	6	9	10	7
December	TBA	11	6	3	7
TOTAL	10	88	84	56	65

CVE

Definición

HOME > CVE > SEARCH RESULTS

Linux kernel 6.13

Search Results

There are **8495** CVE Records that match your search.

Name	
CVE-2025-21703	In the Linux kernel, the following vulnerability has been resolved: netem: Update
CVE-2025-21702	In the Linux kernel, the following vulnerability has been resolved: pfifo_tail_enqu relationship. Let's say Qdisc_A's type is `hfsc`. Enqueue packet to this qdisc will
CVE-2025-21701	In the Linux kernel, the following vulnerability has been resolved: net: avoid race unregister_netdevice_many_notify might run before the rtnl lock section of ethn

resolved

Vendor Linux — **Product** Linux

Versions 1 Total

Default Status: *unaffected*

Affected

- affected from 6.12.5 before 6.12.11

References 2 Total

- https://git.kernel.org/stable/c/d0fb5741932b831eded49bfaaf33353e96200d6d
- https://git.kernel.org/stable/c/fe4de594f7a2e9bc49407de60fbd20809fad4192

CVE-2025-21679 PUBLISHED — View JSON | User Guide

Collapse all

Required CVE Record Information

CNA: kernel.org

Published: 2025-01-31 **Updated:** 2025-01-31

Title: Btrfs: Add The Missing Error Handling Inside Get_canonical_dev_path

Description

In the Linux kernel, the following vulnerability has been resolved: btrfs: add the missing error handling inside get_canonical_dev_path Inside function get_canonical_dev_path(), we call d_path() to get the final device path. But d_path() can return error, and in that case the next strscpy() call will trigger an invalid memory access. Add back the missing error handling for d_path().

Product Status

Learn more

Vendor Linux — **Product** Linux

Versions 2 Total

Default Status: *unaffected*

Affected

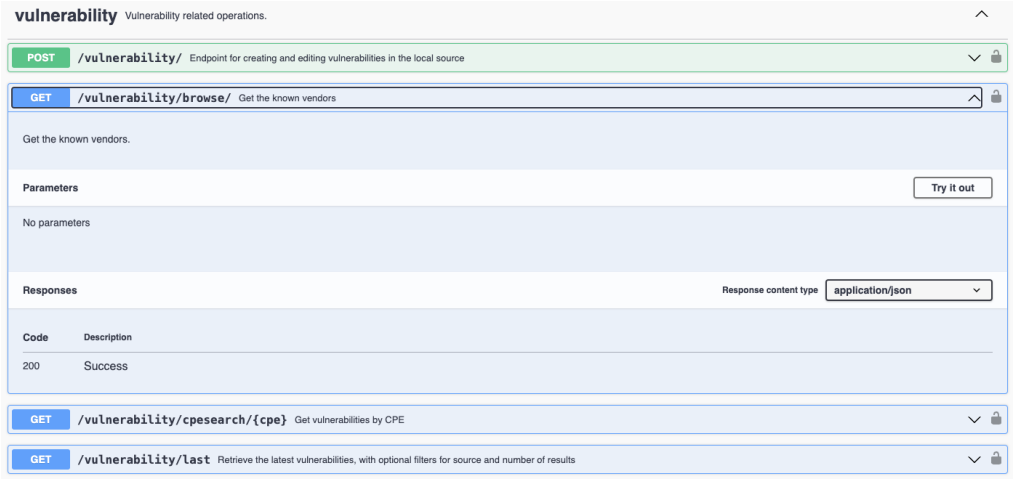
- affected from 5d261f60b5c82ba1e4b5555252e1c90c43d96015 before d0fb5741932b831eded49bfaa
- affected from 7e06de7c83a746e58d4701e013182af133395188 before fe4de594f7a2e9bc49407de60f

CVE

Definición

API Rest

- Existen varias formas de consultar la BD del CVE usando un API que nos permitiria construer aplicaciones que usen la BD.
- Una de las opciones es
  - https://cve.circl.lu/api/
  - Este sitio tiene además más información como estadísticas.



Exploits

Definiciones

Exploits

Definición

- **Fortinet**. An exploit (in its noun form) is a segment of code or a program that maliciously takes advantage of vulnerabilities or security flaws in software or hardware to infiltrate and initiate a denial-of-service (DoS) attack or install malware.
  - The exploit is not the malware itself but is used to deliver the malware. To exploit (in its verb form) is to successfully carry out such an attack.
  - When developers produce software, bugs often appear due to inherent imperfections. These bugs can create a vulnerability in the system, and an exploit searches out such vulnerabilities and looks for a way to exploit databases and networks or systems.
- **Cisco**. An exploit is a program, or piece of code, designed to find and take advantage of a security flaw or vulnerability in an application or computer system, typically for malicious purposes such as installing malware.
  - Types of exploits:
    - Known exploits, Unknown exploits.
    - Hw, Sw, Network (remote, local), etc.
- Otras: https://www.malwarebytes.com/exploits

Exploits

Definición

- Many exploits are designed to provide superuser-level access to a computer system.
- Attackers may use **multiple exploits** in succession to first gain low-level access and then escalate privileges repeatedly until they reach the highest administrative level, often referred to as "root."
- This technique of chaining several exploits together to perform a single attack is known as an exploit chain.

Exploits

Definición

Exploit Database

- The Exploit Database is maintained by OffSec, an information security training company that provides various Information Security Certifications as well as high end penetration testing services.
- The Exploit Database is a non-profit project that is provided as a public service by OffSec.
- The Exploit Database is a CVE compliant archive of public exploits and corresponding vulnerable software, developed for use by penetration testers and vulnerability researchers.
- URL
  - https://www.exploit-db.com/
  - 46,102 exploits (19/feb./2025)

Exploits

Definición

```
# Exploit Title: Pluck CMS 4.7.16 - Remote Code Execution (RCE) (Authentic
# Date: 13.03.2022
# Exploit Author: Ashish Koli (Shikari)
# Vendor Homepage: https://github.com/pluck-cms/pluck
# Version: 4.7.16
# Tested on Ubuntu 20.04.3 LTS
# CVE: CVE-2022-26965
# Usage : python3 exploit.py <IP> <Port> <Password> <Pluckcmspath>
# Example:  python3 exploit.py 127.0.0.1 80 admin /pluck
# Reference: https://github.com/shikari00007/Pluck-CMS-Pluck-4.7.16-Theme-

'''
Description:
A theme upload functinality in Pluck CMS before 4.7.16 allows an admin
privileged user to gain access in the host through the "themes files",
which may result in remote code execution.
'''


'''
Import required modules:
'''
import sys
import requests
import json
import time
import urllib.parse
import struct

'''
User Input:
'''
target_ip = sys.argv[1]
target_port = sys.argv[2]
password = sys.argv[3]
pluckcmspath = sys.argv[4]
```

EXPLOIT DATABASE

EXPLOITS

GHDB

PAPERS

SHELLCODES

SEARCH EDB

SEARCHSPLOIT MANUAL

SUBMISSIONS

ONLINE TRAINING

Pluck CMS 4.7.16 - Remote Code Execution (RC

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
50826	2022-26965	ASHISH KOLI	WEBAPPS	PHP	2022-03-1

EDB Verified: ×

Exploit: ⬇ / {}

Vulnerable App:

EXPLOIT DATABASE

Verified Has App Filters Reset All

Show 15 Search:

Date	D	A	V	Title	Type	Platform	Author
2022-03-16	⬇		×	Apache APISIX 2.12.1 - Remote Code Execution (RCE)	Remote	Multiple	Ven3xy
2022-03-16	⬇		×	Tiny File Manager 2.4.6 - Remote Code Execution (RCE)	WebApps	PHP	FEBIN MON SAJI
2022-03-16	⬇		×	Hikvision IP Camera - Backdoor	Remote	Hardware	Sobhan Mahmoodi

Herramientas

Ejemplos

Herramientas

Software

Algunas de las más utilizadas:

1. Escáneres de Vulnerabilidades
    i. Detección de CVEs en Infraestructura.
    ii. Ejemplo: Nessus, OpenVAS, Rapid7 Nexpose, etc.
2. Herramientas de Evaluación de Seguridad de Sistemas
    i. Ejemplo: Metasploit Framework, DefectDojo, etc.
3. Busca vulnerabilidades en las dependencias (librerías) de un programa.
    i. https://owasp.org/www-project-dependency-check/

Herramientas

Intro

Las que usan los exploits:

1. Metasploit
   - Version comercial
     https://www.rapid7.com/db/
   - Versón gratuita
     https://www.metasploit.com/download

The end

Contacto

Raúl Acosta Bermejo

http:www.cic.ipn.mx
http://www.ciseg.cic.ipn.mx/

racostab@ipn.mx
racosta@cic.ipn.mx

57-29-60-00
Ext. 56652