



Analyse nessus et openvas sur metasploitable3

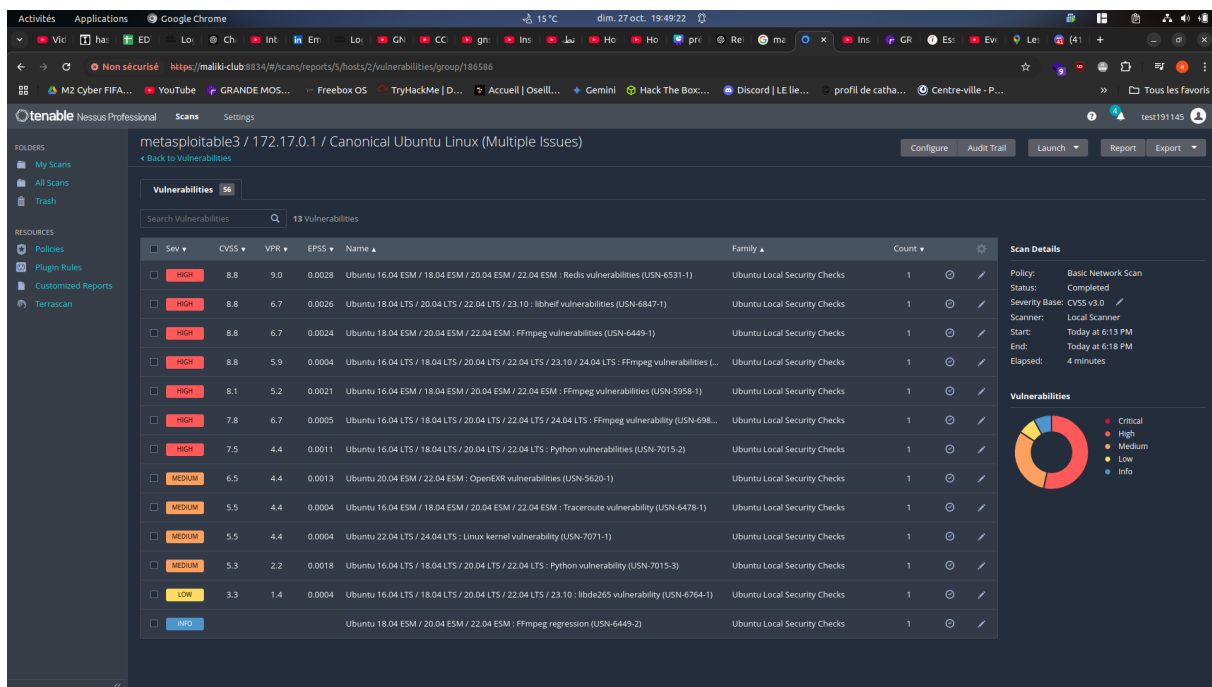
Abdel-malik fofana

Voici la machine que nous allons scanner , une machine metasploitable3 avec l'ip : 172.16.39.128

```
loadkeys: could not deallocate keymap 128
vagrant@ubuntu:~$ sudo loadkeys fr
Loading fr
vagrant@ubuntu:~$ loadkeys fr^C
vagrant@ubuntu:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data:
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=9.46 ms
^C
--- 8.8.8.8 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 9.463/9.463/9.463/0.000 ms
vagrant@ubuntu:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:b0:8d:6d brd ff:ff:ff:ff:ff:ff
    inet 172.16.39.128/24 brd 172.16.39.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:feb0:8d6d/64 scope link
        valid_lft forever preferred_lft forever
3: docker0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:1b:7a:02:9a brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
        valid_lft forever preferred_lft forever
    inet6 fe80::42:1bff:fe7a:29a/64 scope link
        valid_lft forever preferred_lft forever
5: veth180925: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master docker0 state UP group default
    link/ether 76:c2:8e:c0:9a:81 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::74c2:8eff:fec0:9a81/64 scope link
        valid_lft forever preferred_lft forever
vagrant@ubuntu:~$
```

NESSUS scan metasploit

On peut voir que notre machine metasploitable3 a beaucoup de vulnérabilité critique



metasploitable3 / 172.17.0.1 / Canonical Ubuntu Linux (Multiple Issues)

13 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count
HIGH	8.8	9.0	0.0028	Ubuntu 16.04 ESM / 18.04 ESM / 20.04 ESM / 22.04 ESM : Redis vulnerabilities (USN-6531-1)	Ubuntu Local Security Checks	1
HIGH	8.8	6.7	0.0026	Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : libheif vulnerabilities (USN-6847-1)	Ubuntu Local Security Checks	1
HIGH	8.8	6.7	0.0024	Ubuntu 18.04 ESM / 20.04 ESM / 22.04 ESM : FFmpeg vulnerabilities (USN-6449-1)	Ubuntu Local Security Checks	1
HIGH	8.8	5.9	0.0004	Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : FFmpeg vulnerabilities (USN-6449-1)	Ubuntu Local Security Checks	1
HIGH	8.1	5.2	0.0021	Ubuntu 16.04 ESM / 18.04 ESM / 20.04 ESM / 22.04 ESM : FFmpeg vulnerabilities (USN-5958-1)	Ubuntu Local Security Checks	1
HIGH	7.8	6.7	0.0005	Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : FFmpeg vulnerability (USN-698-1)	Ubuntu Local Security Checks	1
HIGH	7.5	4.4	0.0011	Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS : Python vulnerabilities (USN-7015-2)	Ubuntu Local Security Checks	1
MEDIUM	6.5	4.4	0.0013	Ubuntu 20.04 ESM / 22.04 ESM : OpenEXR vulnerabilities (USN-5620-1)	Ubuntu Local Security Checks	1
MEDIUM	5.5	4.4	0.0004	Ubuntu 16.04 ESM / 18.04 ESM / 20.04 ESM / 22.04 ESM : Traceroute vulnerability (USN-6478-1)	Ubuntu Local Security Checks	1
MEDIUM	5.5	4.4	0.0004	Ubuntu 22.04 LTS / 24.04 LTS : Linux kernel vulnerability (USN-7071-1)	Ubuntu Local Security Checks	1
MEDIUM	5.3	2.2	0.0018	Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS : Python vulnerability (USN-7015-3)	Ubuntu Local Security Checks	1
LOW	3.3	1.4	0.0004	Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : libde265 vulnerability (USN-6764-1)	Ubuntu Local Security Checks	1
INFO				Ubuntu 18.04 ESM / 20.04 ESM / 22.04 ESM : FFmpeg regression (USN-6449-2)	Ubuntu Local Security Checks	1

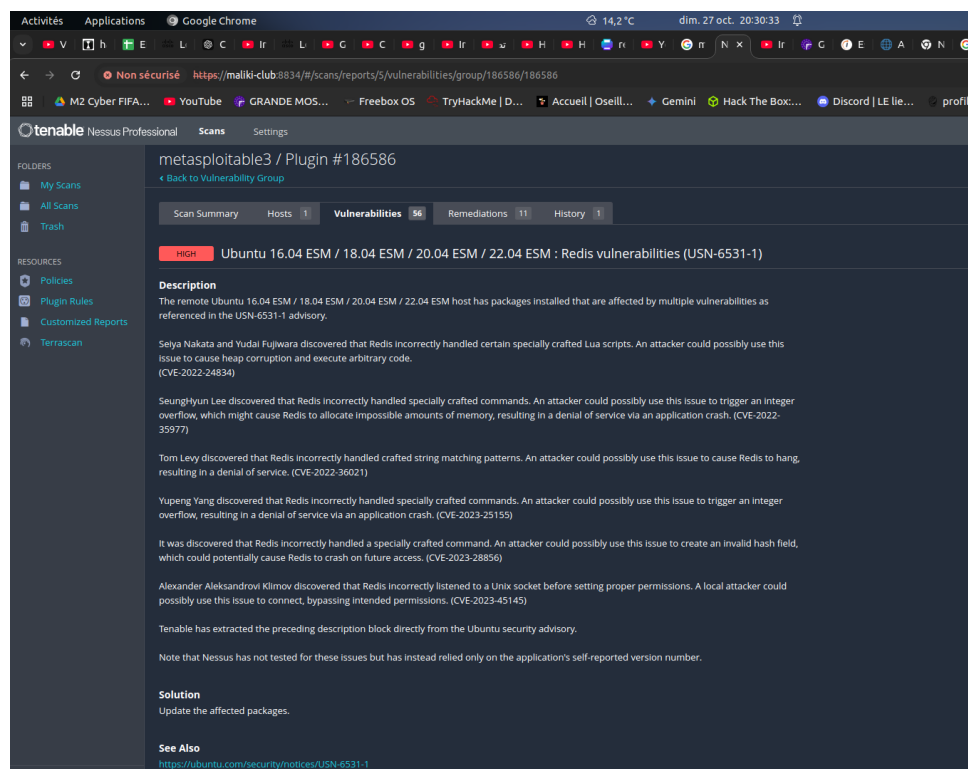
Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 6:18 PM
End: Today at 6:18 PM
Elapsed: 4 minutes

Vulnerabilities

Donut chart showing severity distribution: Critical (red), High (orange), Medium (yellow), Low (green), Info (blue).

Voici une des vulnérabilités



metasploitable3 / Plugin #186586

Scan Summary | Hosts: 1 | Vulnerabilities: 56 | Remediations: 11 | History: 1

HIGH Ubuntu 16.04 ESM / 18.04 ESM / 20.04 ESM / 22.04 ESM : Redis vulnerabilities (USN-6531-1)

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM / 20.04 ESM / 22.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6531-1 advisory.

Selya Nakata and Yudai Fujiwara discovered that Redis incorrectly handled certain specially crafted Lua scripts. An attacker could possibly use this issue to cause heap corruption and execute arbitrary code. (CVE-2022-24834)

SeungHyun Lee discovered that Redis incorrectly handled specially crafted commands. An attacker could possibly use this issue to trigger an integer overflow, which might cause Redis to allocate impossible amounts of memory, resulting in a denial of service via an application crash. (CVE-2022-35977)

Tom Levy discovered that Redis incorrectly handled crafted string matching patterns. An attacker could possibly use this issue to cause Redis to hang, resulting in a denial of service. (CVE-2022-36021)

Yupeng Yang discovered that Redis incorrectly handled specially crafted commands. An attacker could possibly use this issue to trigger an integer overflow, resulting in a denial of service via an application crash. (CVE-2023-25155)

It was discovered that Redis incorrectly handled a specially crafted command. An attacker could possibly use this issue to create an invalid hash field, which could potentially cause Redis to crash on future access. (CVE-2023-28856)

Alexander Aleksandrov Kimov discovered that Redis incorrectly listened to a Unix socket before setting proper permissions. A local attacker could possibly use this issue to connect, bypassing intended permissions. (CVE-2023-45145)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Update the affected packages.

See Also

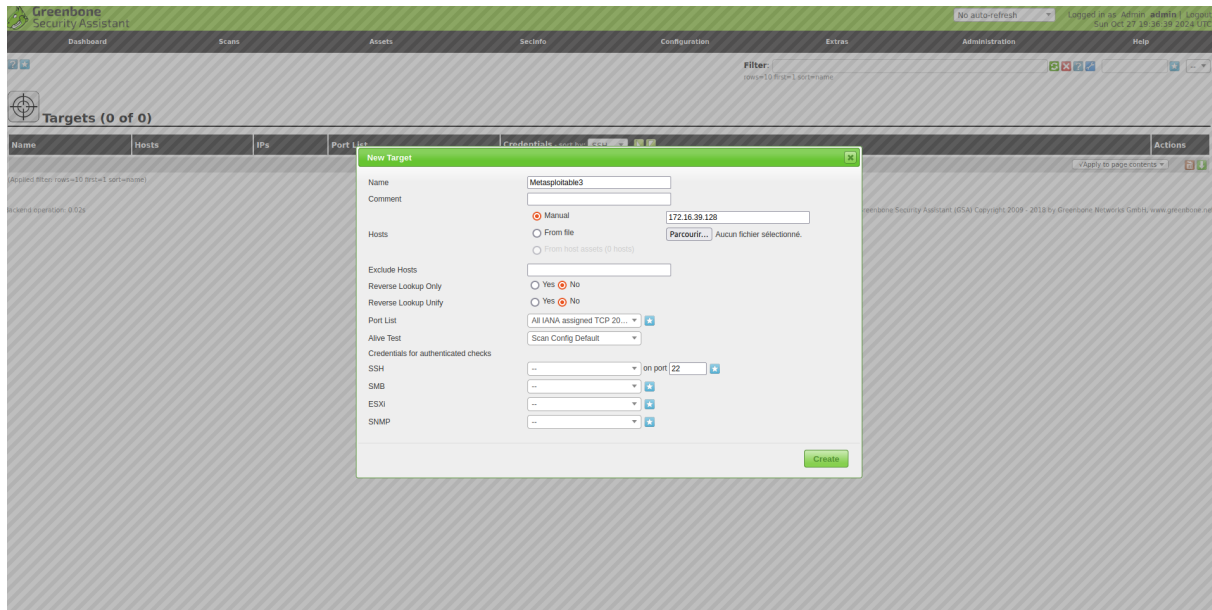
<https://ubuntu.com/security/notices/USN-6531-1>

Voici le lien du rapport nessus :

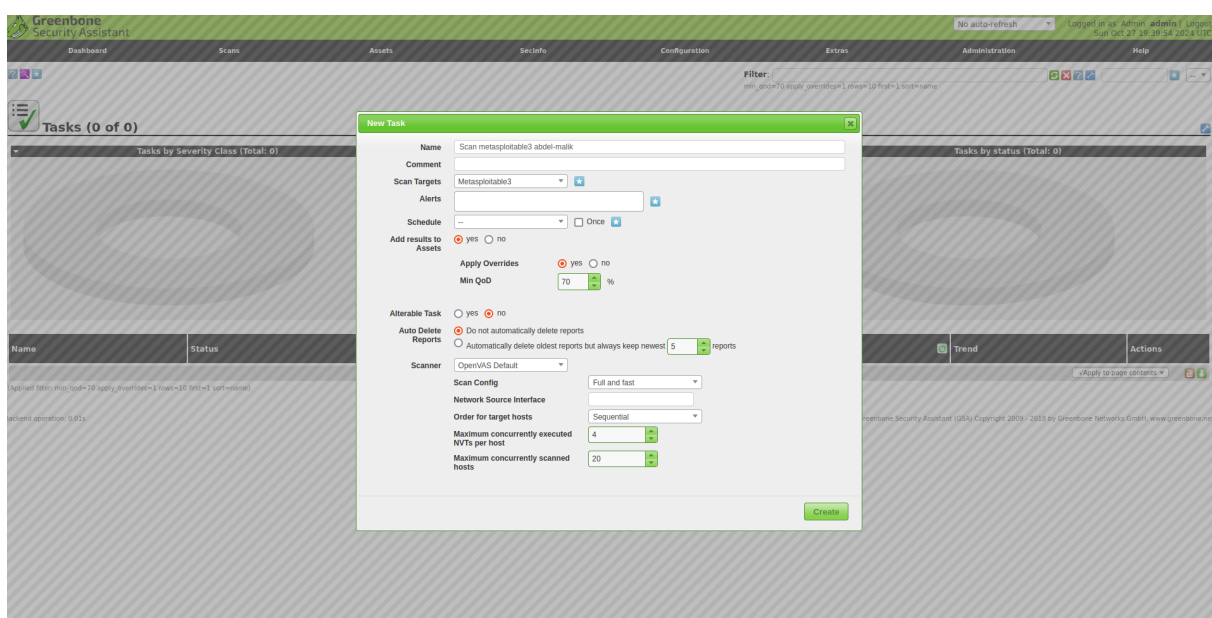
<https://drive.google.com/file/d/1b9YP1yKUXuznAgxlvNPgyNFnrzeaXWQg/view?usp=sharing>

OPENVAS

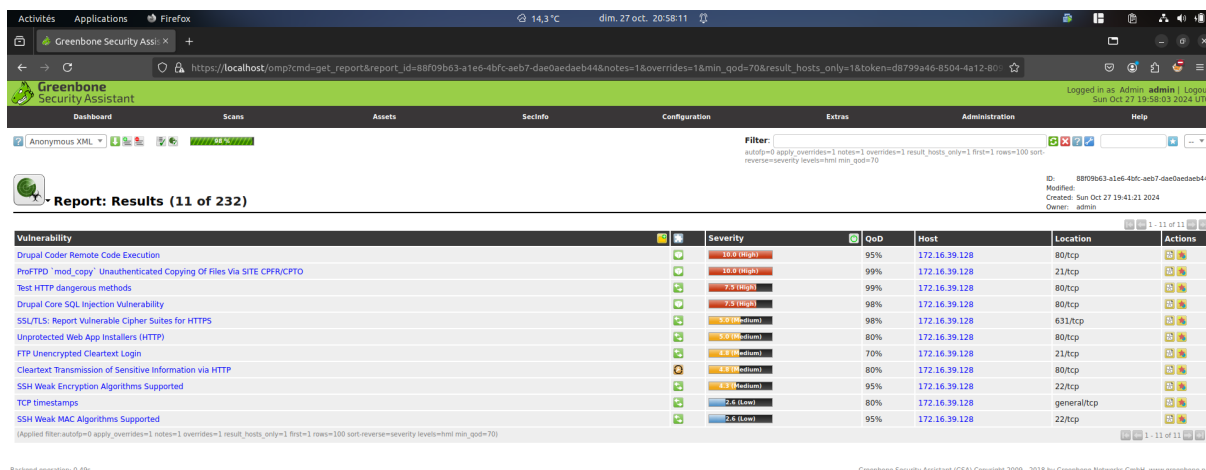
On ajoute notre target



En suite on crée une nouvelle tache en choisissant bien la bonne target



Et on a plein d'erreur critique comme on peut le voir ici



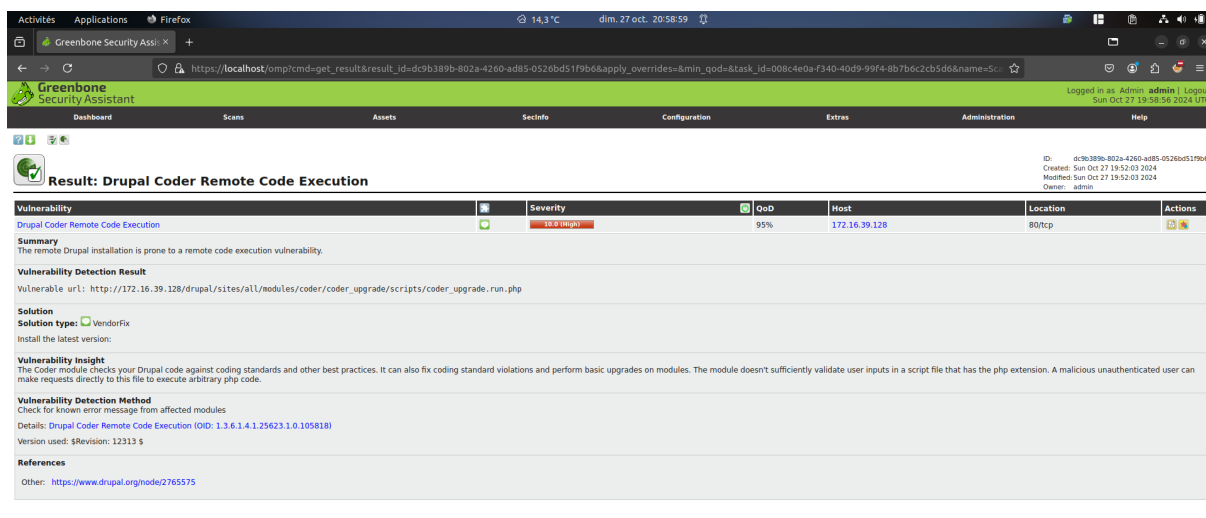
Report: Results (11 of 232)

Vulnerability	Severity	QoD	Host	Location	Actions
Drupal Codex Remote Code Execution	10.0 (High)	95%	172.16.39.128	80/tcp	[Details] [Export]
ProFTPd 'mod_copy' Unauthenticated Copying Of Files Via SITE CPFR/CPFO	10.0 (High)	99%	172.16.39.128	21/tcp	[Details] [Export]
Test HTTP dangerous methods	7.5 (High)	99%	172.16.39.128	80/tcp	[Details] [Export]
Drupal Core SQL Injection Vulnerability	7.5 (High)	98%	172.16.39.128	80/tcp	[Details] [Export]
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	5.0 (Medium)	98%	172.16.39.128	631/tcp	[Details] [Export]
Unprotected Web App Installers (HTTP)	5.0 (Medium)	80%	172.16.39.128	80/tcp	[Details] [Export]
FTP Unencrypted Cleartext Login	5.0 (Medium)	70%	172.16.39.128	21/tcp	[Details] [Export]
Cleartext Transmission of Sensitive Information via HTTP	5.0 (Medium)	80%	172.16.39.128	80/tcp	[Details] [Export]
SSH Weak Encryption Algorithms Supported	4.0 (Medium)	95%	172.16.39.128	22/tcp	[Details] [Export]
TCP timestamps	2.5 (Low)	80%	172.16.39.128	general/tcp	[Details] [Export]
SSH Weak MAC Algorithms Supported	2.5 (Low)	95%	172.16.39.128	22/tcp	[Details] [Export]

Backend operation: 0.49s

Greenbone Security Assistant (GSA) Copyright 2009 - 2018 by Greenbone Networks GmbH, www.greenbone.net

Et on a plein d'information sur la CVE comment resoudre la vulnerabilite etc....



Result: Drupal Codex Remote Code Execution

Vulnerability
Drupal Codex Remote Code Execution

Summary
The remote Drupal installation is prone to a remote code execution vulnerability.

Vulnerability Detection Result
Vulnerable url: http://172.16.39.128/drupal/sites/all/modules/coder/coder_upgrade/scripts/coder_upgrade.run.php

Solution
Solution type: ☐ VendorFix
Install the latest version:

Vulnerability Insight
The Coder module checks your Drupal code against coding standards and other best practices. It can also fix coding standard violations and perform basic upgrades on modules. The module doesn't sufficiently validate user inputs in a script file that has the php extension. A malicious unauthenticated user can make requests directly to this file to execute arbitrary php code.

Vulnerability Detection Method
Check for known error message from affected modules
Details: Drupal Codex Remote Code Execution (OID: 1.3.6.1.4.1.25623.1.0.105818)
Version used: \$Revision: 12313 \$

References
Other: <https://www.drupal.org/node/2765575>

Voici le lien du rapport generer par openvas :

https://drive.google.com/file/d/12r5kT_AYCKln5NiBSrg0z69Wz8yRv2cg/view?usp=sharing