

REMEDIATION META

Apache PHP-CGI Remote Code Execution.....2
SSL Version 2 and 3 Protocol Detection.....3

Apache PHP-CGI Remote Code Execution

Questa vulnerabilità consente l'esecuzione di codice arbitrario su server che utilizzano **PHP-CGI** in combinazione con **Apache**. È causata da una cattiva gestione degli argomenti di linea di comando (*query string*) da parte di PHP quando eseguito tramite **mod_cgi** o **mod_fastcgi**.

Un attaccante può sfruttare questa falla per eseguire comandi di sistema inviando richieste HTTP malformate al server web, ottenendo potenzialmente **accesso completo** al sistema.

L'attaccante può inviare richieste come:

http://vulnerable-server/index.php?-s

Questo comando forza PHP a mostrare il codice sorgente dei file **.php** o eseguire comandi arbitrari con l'utente di Apache (**www-data**).

L'attaccante può lanciare comandi shell (**ls, cat /etc/passwd, ecc.**), avendo accesso completo ai dati sensibili del server.

La soluzione consigliata è **rimuovere completamente php-cgi** e configurare il server per utilizzare **mod_php**, che non è affetto da questa vulnerabilità.

Comando per rimuovere php-cgi su Metasploitable:

sudo apt-get remove php5-cgi

```
msfadmin@metasploitable:~$ sudo apt-get remove php5-cgi
[sudo] password for msfadmin:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages will be REMOVED:
  php5-cgi
0 upgraded, 0 newly installed, 1 to remove and 152 not upgraded.
After this operation, 10.6MB disk space will be freed.
Do you want to continue [Y/n]?
(Reading database ... 37634 files and directories currently installed.)
Removing php5-cgi ...
msfadmin@metasploitable:~$
```

Questa azione elimina l'interprete PHP-CGI, prevenendo così l'esposizione del server a questo tipo di attacco.

SSL Version 2 and 3 Protocol Detection

La vulnerabilità **SSL Version 2 and 3 Protocol Detection** significa che il server supporta ancora i protocolli **SSLv2** e **SSLv3**, entrambi considerati **obsoleti e insicuri**, soggetti a numerosi attacchi noti, come **POODLE** per **SSLv3**.

Per risolvere la vulnerabilità andiamo a modificare il file di configurazione SSL con:

```
sudo nano /etc/apache2/mods-available/ssl.conf
```

Modificando la direttiva “SSLProtocol” con “TLSv1.2” per essere più sicuri.

```
# List the ciphers that the client is permitted to negotiate.
# See the mod_ssl documentation for a complete list.
#SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
# enable only secure ciphers:
#SSLCipherSuite HIGH:MEDIUM:!ADH

# enable only secure protocols: SSLv3 and TLSv1, but not SSLv2
#SSLProtocol all -SSLv1.2

</IfModule>
```

Salviamo il file, e riavviamo Apache con:

```
sudo service apache2 restart
```

Da Kali andiamo a controllare lo stato della porta 443 con:

```
nmap --script ssl-enum-ciphers -p 443 192.168.50.101
```

```
(kali㉿kali)-[~]
└─$ nmap --script ssl-enum-ciphers -p 443 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-09 16:45 CET
Nmap scan report for 192.168.50.101
Host is up (0.0035s latency).

PORT      STATE SERVICE
443/tcp   closed https
MAC Address: 08:00:27:B2:F5:BD (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.68 seconds
```

La porta 443 per i servizi HTTPS risulta chiusa, il che significa che Apache non è configurato per i servizi HTTPS.

