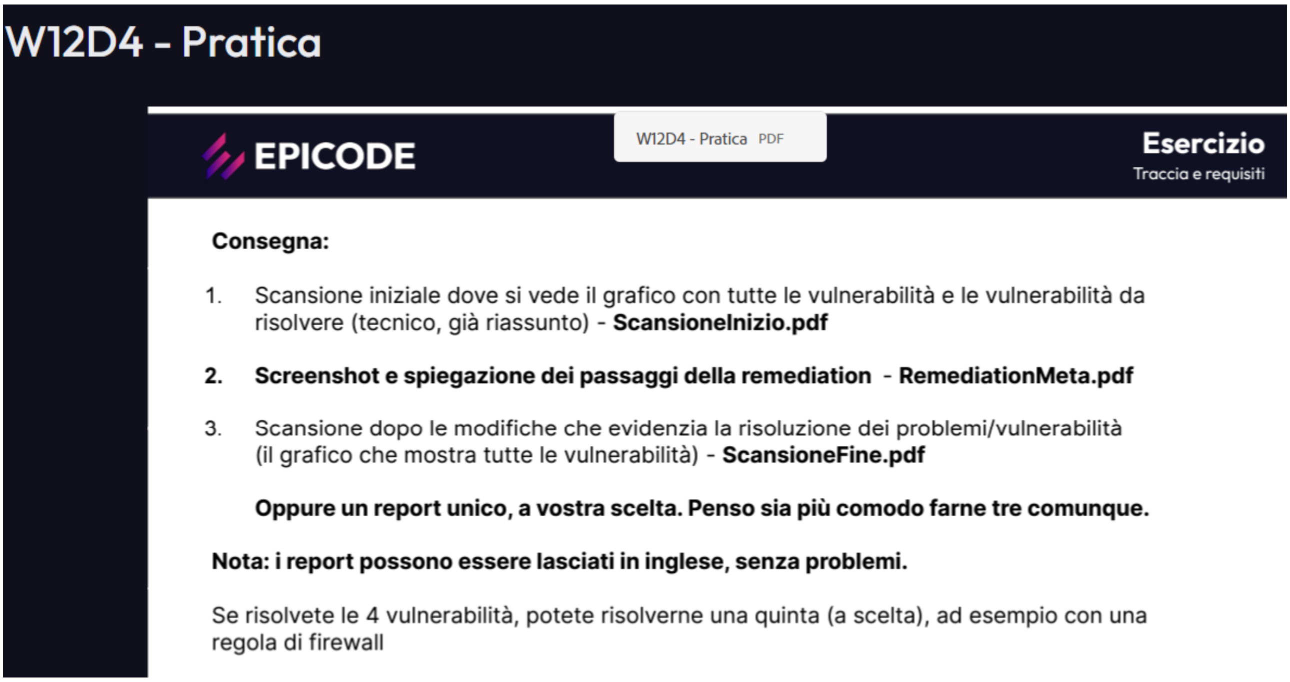


W12D4 - Pratica

Esercizio
Traccia e requisiti

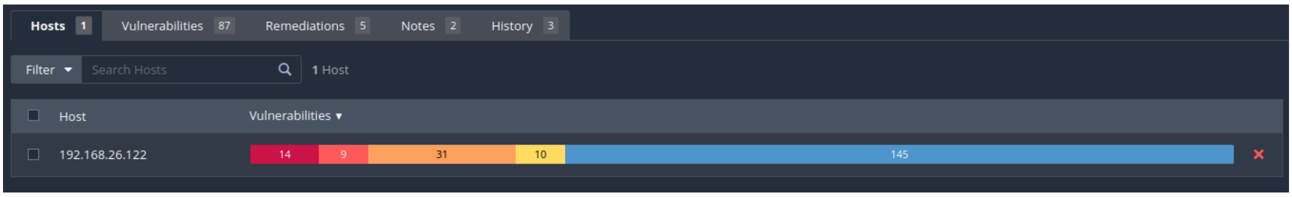
Consegna:

1. Scansione iniziale dove si vede il grafico con tutte le vulnerabilità e le vulnerabilità da risolvere (tecnico, già riassunto) - **ScansioneInizio.pdf**
2. **Screenshot e spiegazione dei passaggi della remediation - RemediationMeta.pdf**
3. Scansione dopo le modifiche che evidenzia la risoluzione dei problemi/vulnerabilità (il grafico che mostra tutte le vulnerabilità) - **ScansioneFine.pdf**

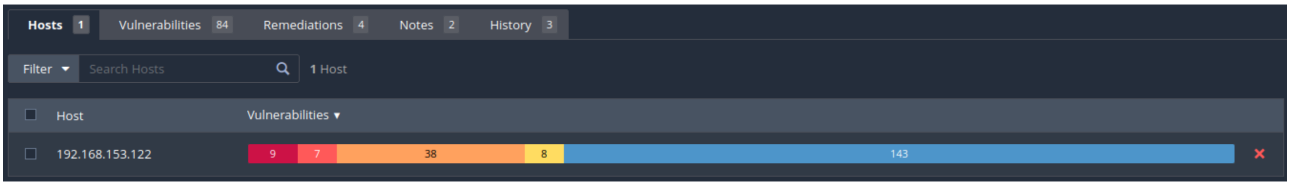
   Oppure un report unico, a vostra scelta. Penso sia più comodo farne tre comunque.

Nota: i report possono essere lasciati in inglese, senza problemi.

Se risolvete le 4 vulnerabilità, potete risolverne una quinta (a scelta), ad esempio con una regola di firewall

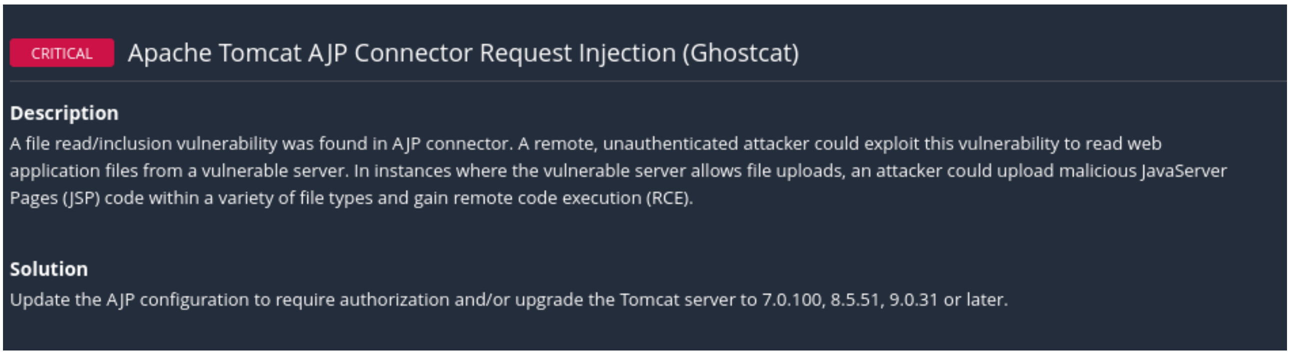


□ Host	Vulnerabilities ▾
□ 192.168.26.122	14 | 9 | 31 | 10 | 145 ✕



□ Host	Vulnerabilities ▾
□ 192.168.153.122	9 | 7 | 38 | 8 | 143 ✕

1 VULNERABILITA'



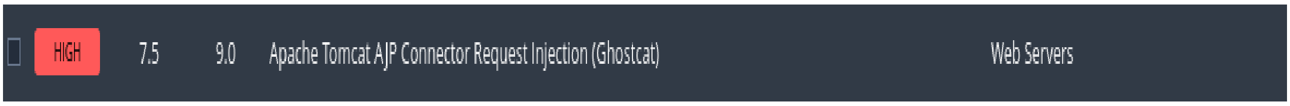
CRITICAL Apache Tomcat AJP Connector Request Injection (Ghostcat)

Description

A file read/inclusion vulnerability was found in AJP connector. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and gain remote code execution (RCE).

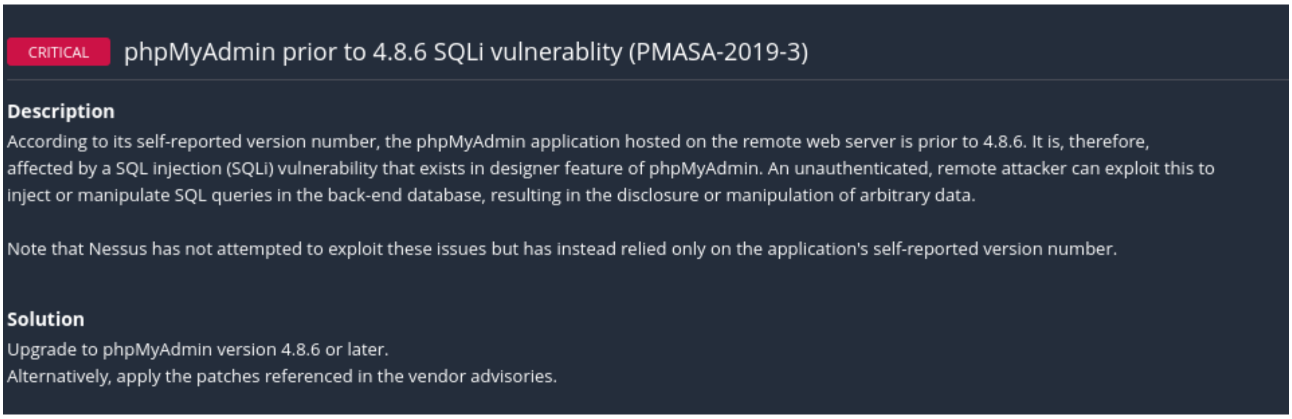
Solution

Update the AJP configuration to require authorization and/or upgrade the Tomcat server to 7.0.100, 8.5.51, 9.0.31 or later.



□ HIGH 7.5 9.0 Apache Tomcat AJP Connector Request Injection (Ghostcat) Web Servers

2 VULNERABILITA’



CRITICAL phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)

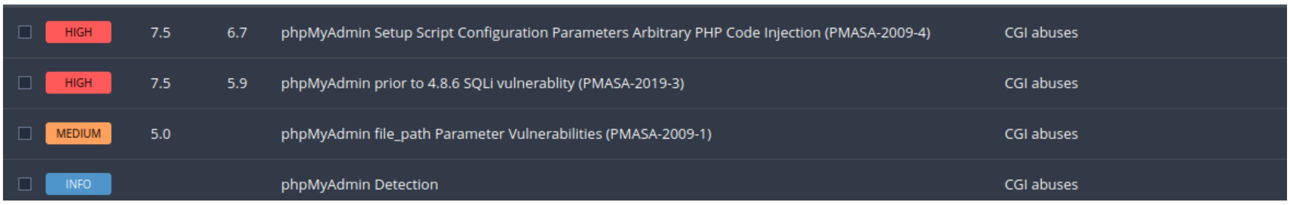
Description

According to its self-reported version number, the phpMyAdmin application hosted on the remote web server is prior to 4.8.6. It is, therefore, affected by a SQL injection (SQLi) vulnerability that exists in designer feature of phpMyAdmin. An unauthenticated, remote attacker can exploit this to inject or manipulate SQL queries in the back-end database, resulting in the disclosure or manipulation of arbitrary data.

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

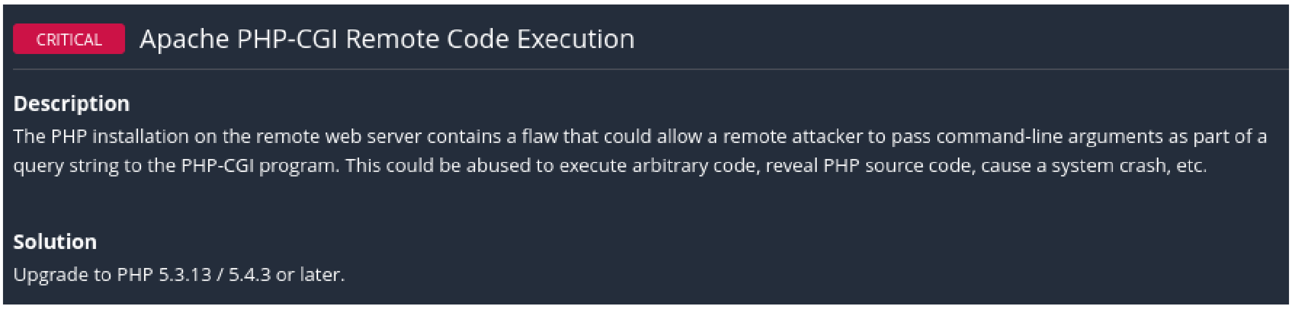
Solution

Upgrade to phpMyAdmin version 4.8.6 or later.
Alternatively, apply the patches referenced in the vendor advisories.



□	HIGH	7.5	6.7	phpMyAdmin Setup Script Configuration Parameters Arbitrary PHP Code Injection (PMASA-2009-4)	CGI abuses
□	HIGH	7.5	5.9	phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)	CGI abuses
□	MEDIUM	5.0		phpMyAdmin file_path Parameter Vulnerabilities (PMASA-2009-1)	CGI abuses
□	INFO			phpMyAdmin Detection	CGI abuses

3 VULNERABILITA’



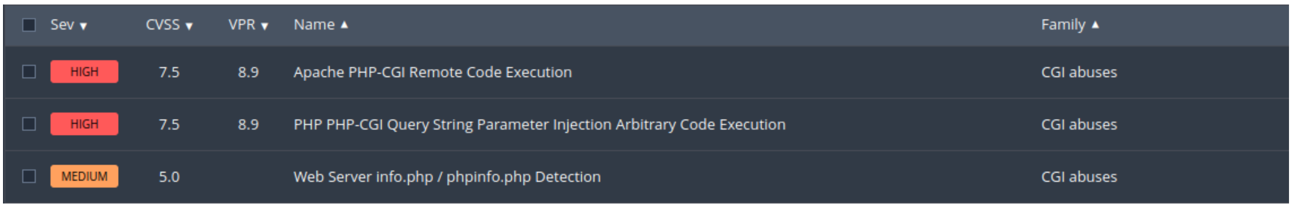
CRITICAL Apache PHP-CGI Remote Code Execution

Description

The PHP installation on the remote web server contains a flaw that could allow a remote attacker to pass command-line arguments as part of a query string to the PHP-CGI program. This could be abused to execute arbitrary code, reveal PHP source code, cause a system crash, etc.

Solution

Upgrade to PHP 5.3.13 / 5.4.3 or later.



□	Sev ▾	CVSS ▾	VPR ▾	Name ▲	Family ▲
□	HIGH	7.5	8.9	Apache PHP-CGI Remote Code Execution	CGI abuses
□	HIGH	7.5	8.9	PHP PHP-CGI Query String Parameter Injection Arbitrary Code Execution	CGI abuses
□	MEDIUM	5.0		Web Server info.php / phpinfo.php Detection	CGI abuses