CP3414 Assessment 3

Vulnerability Analysis Report

Pyae Sone Soe Moe

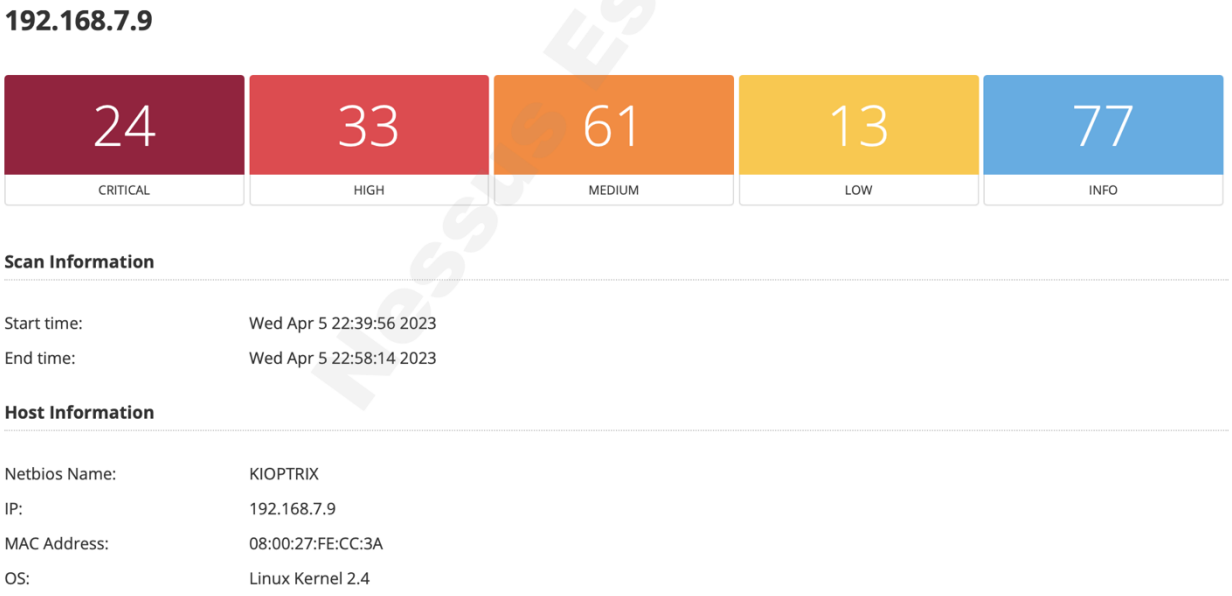
ID – 14039156

Executive Summary

Critical vulnerabilities in Apache 2.4.x were found during the scan of IP address 192.168.7.9, underscoring the urgency of taking urgent action to upgrade to Apache 2.4.53, perform routine patching, and implement security measures. Prior to 1.3.27, there were high-risk vulnerabilities in Apache versions that also require immediate attention. These vulnerabilities require updates, particular threat protection, and buffer overflow patch implementation. Suggestions include regular scanning, upgrading to the most recent versions of Apache, and ongoing monitoring to guarantee strong security. Singular vulnerabilities were found for the other hosts (192.168.7.8, 192.168.7.7, and 192.168.7.6), necessitating customized mitigating measures. Constant watchfulness and methodical updates are essential for a strong and reliable security posture.

Technical Findings

192.168.7.9



For the IP **192.168.7.9** we were able to detect 24 critical, 33 high, 61 medium, 13 low and 77 info. Information such as the hostname, IP address, MAC address, and operating system of the scanned host are shown, together with information on the start and end times of the scan. Specifically, the scan ran from 10:39 PM on April 5, 2023, to 10:58 PM. The host under scan has the NetBIOS name KIOPTRIX, a MAC address of 08:00:27:FE:CC:3A, an IP address of 192.168.7.9, and is running Linux Kernel 2.4. This host has 33 major vulnerabilities, which can potentially cause for serious damages. This category of security vulnerabilities is known as critical ones, which increase the chance that an intruder will use them to take over a system or collect data. It is important to quickly identify and fix serious vulnerabilities.

Critical

158900 - Apache 2.4.x < 2.4.53 Multiple Vulnerabilities

Mod_lua Use of Uninitialized Value (CVE-2022-22719)

The potential exploitation of a properly designed request that causes mod_lua to read uninitialized values is a serious reason to concern. The potential of this vulnerability to allow access to random parts of memory offers a risk of the server failing. It is important that this risk to be addressed and mitigated as soon as possible.

HTTP Request Smuggling (CVE-2022-22720)

The server is vulnerable to HTTP request smuggling attacks because it fails to disconnect connections when issues occur. Attackers could be able to use this vulnerability (CVE-2022-22720) to change and compromise the integrity of HTTP requests. Responses must be taken quickly in order to stop this vulnerability from being exploited.

Possible Buffer Overflow (CVE-2022-22721)

The potential of a buffer overflow when the LimitXMLRequestBody is set too high is another significant concern. A data overflow might result from this, which could cause inaccessible writes and, in the most serious situation, possibly even code execution. To mitigate the risk related with this vulnerability, quick action is required to change configurations and set up security measures (CVE-2022-22721).

Read/Write Beyond Bounds in mod_sed (CVE-2022-23943)

A mod_sed vulnerability allows attackers rewrite heap memory with malicious data, exposing the server at risk for security breaches. It is essential to address this vulnerability (CVE-2022-23943) because it can be used for illegal memory changes, which might harm the server's overall security status. Having safeguards in place is essential for preventing this vulnerability from being exploited.

158900 - Apache 2.4.x < 2.4.53 Multiple Vulnerabilities

Impacted System

Web Address: https://192.168.7.9
Software: Apache HTTP Server
Current Version: 1.3.20 (Vulnerable)
Updated Version: 2.4.53 (Secure)

CVE-2022-22719 (mod_lua Use of Uninitialized Value)

This type of vulnerability is a serious threat to the reliability of the system. A carefully planned request can be used to trick the server into reading values that have not been set up, which could lead to a crash through accessing random memory regions. This vulnerability has more consequences than only instability, so it needs to be handled immediately in order to mitigate the risk.

CVE-2022-22720 (HTTP Request Smuggling)

The server shows a serious flaw in connection management, since it does not terminate connections in the case of an error. Because of this vulnerability, attackers may bypass security measures by using the system to launch HTTP request smuggling attacks. There could be serious consequences because this vulnerability could be used to run malicious malware and compromise the server's integrity. For the server to be protected against these clever attacks, urgent remediation is required.

CVE-2022-22721 (Possible Buffer Overflow)

This vulnerability shows the potential risk that comes from overly increasing the LimitXMLRequestBody. An integer overflow caused by this configuration issue may result in inaccessible writing along with, in the worst case, possible code execution. For it to limit the risk and create safeguards against unauthorized code execution, resolving this vulnerability requires a careful change of configurations.

CVE-2022-23943 (Read/Write Beyond Bounds in mod_sed)

This vulnerability shows a significant risk to the server. Due to this mod_sed vulnerability, attackers can use malicious data to overwrite heap memory, compromising the server's overall security. To boost defenses against potential breaches resulting from this particular vulnerability, swift action is required. Effective safety precautions must be put in place to protect the integrity of the server and stop illegal access to important memory locations.

170113 - Apache 2.4.x < 2.4.55 Multiple Vulnerabilities

Impacted System

URL: http://192.168.7.9
Software: Apache HTTP Server
Version: 1.3.20 (Vulnerable)
Fixed Version: 2.4.55 (Secure)

CVE-2006-20001 (Memory Read/Write Overflow)

This memory manipulation vulnerability presents an important risk. Particularly, a carefully designed request header may cause memory corruption and server breakdowns. This vulnerability has broad effects that go beyond simple instability and include serious results like data breaches and code execution. Because Apache versions up to 2.4.54 are affected by this vulnerability, it is essential that the risk be addressed and mitigated in order to avoid the serious consequences that have been highlighted.

CVE-2022-36760 (HTTP Request Smuggling in mod_proxy_ajp)

This vulnerability uses mod_proxy_ajp's HTTP Request Smuggling to provide an important attack pathway. Because of this vulnerability, attackers can get past security measures and send requests to AJP servers that are not allowed. This vulnerability could lead to serious consequences like malware installation, unauthorized access, and data breaches. Understanding the importance of fixing this vulnerability is crucial, especially for Apache versions up to 2.4.54, in order to enhance defenses against the potential threats mentioned.

CVE-2022-37436 (Response Header Truncation)

Due to this vulnerability, there may be a way for malicious back ends to bypass security measures by reducing response headers. This vulnerability has the potential to end up in information exposure, security bypasses, and unwanted access. This vulnerability affects Apache versions 2.4.55 and below, emphasizing the need for quick action to address and reduce the risk of possible security breaches and unauthorized access. Enforcing strong security protocols is crucial to maintaining the reliability of the server's response processing systems.

High

11137 - Apache < 1.3.27 Multiple Vulnerabilities (DoS, XSS)

Impacted System

URL: http://192.168.7.9
Software: Apache HTTP Server
Version: 1.3.20 (Vulnerable)
Fixed Version: 1.3.27 (Secure)

Cross-Site Scripting (XSS) through Unfiltered Host Headers (CVE-2002-0839)

Due to unprocessed host headers, this vulnerability presents a serious risk of Cross-Site Scripting (XSS). By making use of this weakness, attackers can insert malicious code into websites, which may result in the loss of user data, the hijacking of a user's session, or a redirection to phishing websites. Due to the broad impact of this vulnerability, which affects all versions of Apache prior to 1.3.27, mitigation efforts

are important in order to protect against potential compromise and malicious script injection.

Denial-of-Service (DoS) in Apache Scorecard

The Apache Scorecard module has a vulnerability to Denial-of-Service (DoS) attacks. These attacks allow an attacker to take advantage of a weakness and cause the web server to crash. This type of attack results in significant service interruption and downtime. This vulnerability affects all versions of Apache before 1.3.27, and it needs to be fixed immediately in order to strengthen the server's resilience against future failures and guarantee continuous execution of services.

Buffer Overflow in ab.c (CVE-2002-0840)

This vulnerability refers to a buffer overflow within the benchmarking software 'ab.c.' By making use of this vulnerability, attackers can run any code on the server, which could give them complete control and compromise the system. Since this serious risk exists in all versions of Apache prior to 1.3.27, it is essential that it be addressed and patched in order to prevent unauthorized code execution and strengthen the server's overall security posture. Quick repair actions are essential to prevent possible exploitation and lessen the broad consequences linked to this buffer overflow issue.

31654 - Apache < 1.3.37 mod_rewrite LDAP Protocol URL Handling Overflow

Impacted System

URL: http://192.168.7.9
Software: Apache HTTP Server
Version: 1.3.20 (Vulnerable)

Fixed Version: 1.3.37 (Secure)

Type: Off-by-one buffer overflow
Module: mod_rewrite
CVE ID: CVE-2006-3747

Certain patterns in LDAP protocol URLs are processed improperly by the mod_rewrite module, creating an exploitable buffer overflow vulnerability. In order to cause this overflow, attackers can create malicious requests and if they succeed, the server's buffer may overflow, and arbitrary code may be executed.

11030 - Apache Chunked Encoding Remote Overflow

Impacted System

Software: Apache HTTP Server
Versions: 1.2.2 and above, 1.3 through 1.3.24, and 2.0 through 2.0.36
Fixed Versions: 1.3.26 (1.3 branch) and 2.0.39 (2.0 branch)

Buffer Overflow

A buffer overflow occurs as a result of the Apache server handling specially designed divided encoding requests incorrectly. By using this overflow, attackers can insert malicious code and take total control of the system.

192.168.7.8

This host only has a single critical vulnerability which the scan started from Wed Apr 5 22:39:56 2023 and ends at Wed Apr 5 22:42:13 2023 with the use of Microsoft Windows 7 Ultimate operating system.

192.168.7.7

192.168.7.7

Scan Information

Start time:	Wed Apr 5 22:39:56 2023
End time:	Wed Apr 5 22:47:26 2023

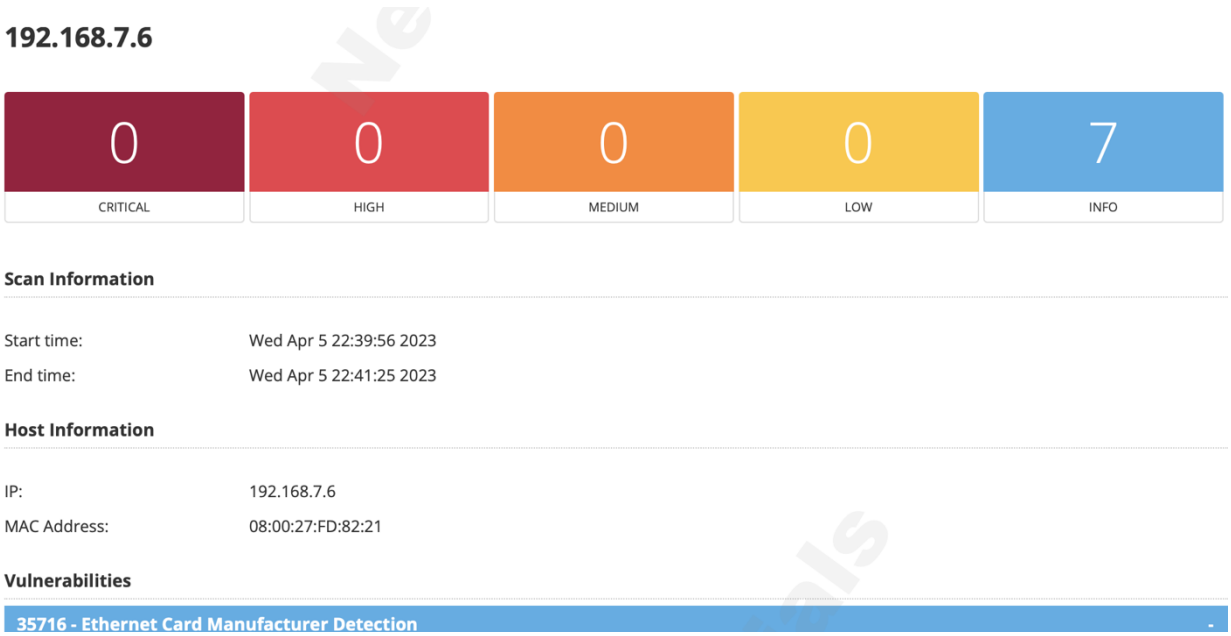
Host Information

IP:	192.168.7.7
MAC Address:	08:00:27:82:2B:92
OS:	Linux Kernel 2.6

Vulnerabilities

This host does contain a single vulnerability which the scan started from Wed Apr 5 22:39:56 2023 and ends at Wed Apr 5 22:47:26 2023 with the use of Linux Kernel 2.6 operating system.

192.168.7.6



192.168.7.6

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	0	0	7

Scan Information

Start time:	Wed Apr 5 22:39:56 2023
End time:	Wed Apr 5 22:41:25 2023

Host Information

IP:	192.168.7.6
MAC Address:	08:00:27:FD:82:21

Vulnerabilities

35716 - Ethernet Card Manufacturer Detection -

This host also does contain a single vulnerability which the scan started from Wed Apr 5 22:39:56 2023 and ends at Wed Apr 5 22:41:25 2023 without the use of proper operating system.

Summary of Findings

Critical Vulnerabilities

Vulnerabilities in mod_lua (CVE-2022-22719), HTTP Request Smuggling (CVE-2022-22720), potential buffer overflow (CVE-2022-22721) and read/write beyond boundaries in mod_sed (CVE-2022-23943) represent severe risks in Apache 2.4.x versions prior to 2.4.53. Implementing protections, patching often, and upgrading to Apache 2.4.53 are all critical steps that must be taken immediately.

Vulnerabilities such as memory read/write overflow (CVE-2006-20001), HTTP Request Smuggling (CVE-2022-36760), and response header truncation (CVE-2022-37436) are still present in Apache 2.4.x versions prior to 2.4.55. It is advised to take immediate action, which includes updating Apache to version 2.4.55, setting up a Web Application Firewall (WAF), and doing routine scans.

High Risk Vulnerabilities

Cross-site scripting (XSS) (CVE-2002-0839), denial-of-service (DoS) in Apache Scorecard, and a buffer overflow in ab.c (CVE-2002-0840) are high-risk vulnerabilities for Apache versions earlier than 1.3.27. It is imperative that you take quick action to fix the buffer overflow, secure against XSS, and upgrade to Apache 1.3.27.

Prior to Apache 1.3.37, there was a mod_rewrite vulnerability (CVE-2006-3747) that requires immediate attention, which includes updating to Apache 1.3.37.

Finally, Apache 1.2.2 and higher, 1.3 through 1.3.24, and 2.0 through 2.0.36 are all impacted by a flaw in chunked encoding handling. To

reduce this risk, immediate action is required, which may include updating to specific versions.

Recommendations

192.168.7.9

In order to mitigate the vulnerabilities found in Apache, a number of preventative measures as well as ongoing efforts are recommended. Firstly, we must immediately update Apache to version 2.4.53 or higher, as this version fixes and patches all known vulnerabilities. Also, it is essential to institute a regular patching procedure to ensure prompt updates for potential future vulnerabilities. It is important to keep track on security alerts for Apache and other relevant software in order to be updated on newly found vulnerabilities and patches. When it is not possible to fix immediately, installing a Web Application Firewall (WAF) can offer a temporary security measure. It is crucial to review and update web application configurations to comply with security best practices. Regular vulnerability scanning also helps in identifying and reducing potential threats.

It is highly recommended to upgrade Apache to version 2.4.55 or later for a thorough and lasting solution. In the meanwhile, putting in place a WAF can provide additional safety against possible intrusions. In order to minimize exploitable vulnerabilities, regular efforts should involve analyzing and updating web application configurations that stick to safe coding guidelines. Finding vulnerabilities and taking serious steps to fix them still depend on conducting regular vulnerability checks. To identify such exploitation attempts, it is essential to keep an eye out for strange activity in server logs and security warnings.

Immediate response that is specific to each situation is encouraged for particular vulnerabilities. In one case, the first priority is to upgrade to Apache version 1.3.27 or the probability of successful exploitation increases dramatically if the upgrade is delayed. Upgrading to version

1.3.37 or later is given comparable priority in another case. When it is not possible to fix right away, setting up a WAF and checking and updating configurations become essential temporary measures. It is still important to keep an eye on security warnings and server logs in order to spot any unusual activity that might point to exploitation efforts. All of these suggestions work together to strengthen Apache servers against possible attacks and guarantee the continuous security of online applications.

References

https://nvd.nist.gov/

https://httpd.apache.org/security_report.html

https://www.sei.cmu.edu/about/divisions/cert/

https://www.cert.org