Amjad Alqahtani

Principles of Cybersecurity

Assignment 1

09/13/2024

Common Vulnerabilities and Exposures

Before answering the questions, I would like to explain what Common Vulnerabilities and Exposures (CVE) are. CVE is a standard used by vendors to identify, list, and define security vulnerabilities in software and systems (reference 1).

Remote Code Execution (RCE)

1. Apache Log4j (CVE-2021-44228)

- Apache Log4j: is a logging tool used in many Java-based applications(reference 2). It allows developers to log and record application events, errors, and other significant runtime information.
- CVE-2021-44228: is a critical vulnerability in Apache Log4j. This vulnerability allows attackers to remotely execute malicious code on a vulnerable system without needing to log in (reference 3).
- Attack Vector: Attackers can exploit the Log4j Vulnerability through multiple vectors:
    1. Web Requests: Malicious requests containing crafted log entries trigger the vulnerability. An attacker constructs a log message with a malicious JNDI lookup, disguising it as a regular log entry. This malicious string is disguised as a regular log entry, which could be sent via various input methods (e.g., HTTP requests, form fields).
    2. Network Protocols: Log messages from network communications can exploit the vulnerability.
    3. Third-party Integrations: Vulnerable libraries or components can introduce the exploit.

    When the vulnerable Log4j library processes the log message, it attempts to resolve the JNDI lookup, inadvertently executing the embedded code. This involves making a request to the attacker's server. The attacker's server responds with malicious code or a reference to malicious code. This execution can lead to remote code execution on the affected system, giving the attacker unauthorized access and control. This vulnerability allows attackers to remotely execute arbitrary code on systems running vulnerable versions of the Log4j library by injecting malicious input into log messages(reference 4) .

- Mitigation: Update to a non-vulnerable version of Log4j (2.16.0 or later), disable lookup features, or apply a temporary fix such as environment variable restrictions.
- However, there are many different responses for mitigation:

1. Apache's Response to the Log4j Vulnerability

    Patch Development and Release:

    1. Code Isolation: Apache identified and isolated the vulnerable sections of code.
    2. Remediation: Applied targeted fixes to address the vulnerability while maintaining functionality.
    3. Quality Assurance: Conducted extensive testing to ensure the patches were effective and stable.

2. Communication with the User Community:

    1. Security Advisory: Released detailed information about the vulnerability, impact, and mitigation steps.
    2. Public Notifications: Issued announcements to raise awareness among users, administrators, and developers.

3. Immediate Actions for Affected Organizations

    Applying Patches and Updates

    1. Patch Installation: Update to the patched versions of Log4j.
    2. Verification: Ensure patches are applied correctly and verify compatibility with existing systems.

4. Assessing and Securing Vulnerable Systems

    1. System Inventory: Identify systems using vulnerable Log4j versions.
    2. Risk Assessment: Evaluate the impact and risks based on system criticality and data sensitivity.

5. Long-Term Lessons and Security Implications

Importance of Thorough Code Reviews and Security Audits

1. Code Review: Regular reviews can help identify and fix security flaws before they become issues.
2. Security Audits: Periodic audits of third-party libraries and dependencies can prevent future vulnerabilities.

2. Microsoft Exchange (CVE-2021-26855)

- Microsoft Exchange is one of the most widely used enterprise email solutions globally. It has recently faced significant security concerns. A discovered exploit, CVE-2021-26855, has been making headlines. This vulnerability allows attackers to gain unauthorized access to a user's email account, potentially enabling them to steal sensitive information or initiate additional attacks.(Reference 5).

- Attack Vector: This vulnerability exploits a Server-Side Request Forgery (SSRF) flaw, enabling an unauthenticated attacker to send crafted HTTP requests, which leads to remote code execution by gaining control of the Exchange server.

  Here are the steps of the CVE-2021-26855 attack vector: (reference 7)
  1. The attacker crafts a POST request to a publicly accessible file (e.g., `/ecp/x.js`) on the Microsoft Exchange server.
  2. The X-BEResource cookie in the request is used to redirect it to an internal service, impersonating an authenticated user, such as an administrator.
  3. The attacker gains access to the Exchange Control Panel (ECP).
  4. From here, they can chain other vulnerabilities (e.g., CVE-2021-26858, CVE-2021-27065) to overwrite files or further exploit the system.

- Mitigation: Apply Microsoft's security patches immediately, restrict access to Exchange services, and implement strong network segmentation to protect internal servers.
- Many responses as follow: (reference 6)
  1. Install the Security Patch: Microsoft recommends installing the security patch as it provides complete mitigation for the vulnerability and does not impact existing functionality.
  2. Interim Mitigation Techniques: If you cannot immediately apply the security patch, use the following interim measures:
     1. IIS Re-Write Rule: Implement this rule to filter out malicious HTTPS requests.
     2. Disable Certain VDirs: Disable Unified Messaging (UM), Exchange Control Panel (ECP) VDir, and Offline Address Book (OAB) VDir. You can apply these changes using the ExchangeMitigation.ps1 script.
     3. Backend Cookie Mitigation: Perform backend cookie mitigation to filter HTTPS requests containing malicious X-AnonResource-Backend and X-BEResource cookies, which are used in SSRF attacks. These measures help protect against the vulnerability until the security patch can be applied.

3. Command Line Execution Cisco Hyperflex (CVE-2021-1497)

A vulnerability in the web-based management interface of Cisco HyperFlex could allow an unauthenticated, remote attacker to perform a command injection attack against an affected device (reference 8).

Attack Vector:

1. The vulnerability allows an attacker to execute arbitrary commands by exploiting improper input validation in the Cisco HyperFlex systems.
2. An attacker sends crafted HTTP requests to the system, bypassing authentication and gaining unauthorized control.
3. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to execute arbitrary commands on an affected device as the root user.

Mitigation:

1. Apply Security Patches: Update to the latest firmware version provided by Cisco.
2. Restrict Network Access: Limit access to the management interface using firewall rules.
3. Monitor Traffic: Set up monitoring for suspicious or unauthorized traffic targeting the system.
4. Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability from the Cisco perspective.

4. Command Injection • Hikvision Web Server (CVE-2021-36260)

A command injection vulnerability in the web server of some Hikvision product. Due to the insufficient input validation, an attacker can exploit the vulnerability to launch a command injection attack by sending some messages with malicious commands.

Attack Vector:
This vulnerability is a command injection flaw in the web server of Hikvision products, where attackers can remotely send crafted messages to execute arbitrary commands with root privileges. The flaw arises from insufficient input validation, allowing attackers to gain control of the device without authentication.

Mitigation (reference 9):

1. Update Firmware: Install the latest firmware patch released by Hikvision in September 2021.
2. Restrict Access: Limit access to the web server interface via firewall rules.
3. Monitor Activity: Watch for unusual network traffic or unauthorized access attempts.

5. Authentication Bypass by Spoofing • Apache (CVE-2022-24112)

This attack-focused weakness is caused by incorrectly implemented authentication schemes that are subject to spoofing attacks.

Attack Vector:

The attack can be done Remotely. This vulnerability allows an attacker to execute arbitrary code on the target Exchange Server via crafted requests. It is primarily exploited over the network, allowing an attacker to remotely compromise the server without needing physical access(reference 10).

Mitigation:

1. Patch Application: The primary mitigation for CVE-2022-24112 is to apply the security updates released by Microsoft.
2. Network Segmentation: Limit exposure of Exchange servers to the internet by using firewalls and network segmentation to reduce the attack surface.
3. Access Controls: Implement strong access controls and least privilege principles for user accounts and services running on the Exchange server.
4. Monitoring: Regularly monitor logs and network traffic for any suspicious activities that could indicate exploitation attempts.

References:

1- https://www.youtube.com/watch?v=cNKDiWH6eOk
2- https://msrc.microsoft.com/blog/2021/12/microsofts-response-to-cve-2021-44228-apache-log4j2/
3- https://www.oracle.com/security-alerts/alert-cve-2021-44228.html#:~:text=Description,for%20a%20username%20and%20password.
4- https://medium.com/@aka.0x4C3DD/log4j-vulnerability-cve-2021-44228-log4shell-a-zero-day-remote-code-execution-exploit-9440cdb1e771

5- https://medium.com/@khadraoui.chouaib/vulnerabilities-in-microsoft-exchange-how-to-mitigate-the-cve-2021-26855-exploit-4af1f9c4a91a
6- https://medium.com/@urshilaravindran/microsoft-exchange-ssrf-cve-2021-26855-b848d757f1d5

7- https://bi-zone.medium.com/hunting-down-ms-exchange-attacks-part-1-proxylogon-cve-2021-26855-26858-27065-26857-6e885c5f197c
8- https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-hyperflex-rce-TjjNrkpR.html
9- https://www.twingate.com/blog/tips/cve-2021-36260
10- https://www.cvedetails.com/cve/CVE-2022-24112/