Mitigation Planning of Vulnerabilities in LumipOne by VulnHub

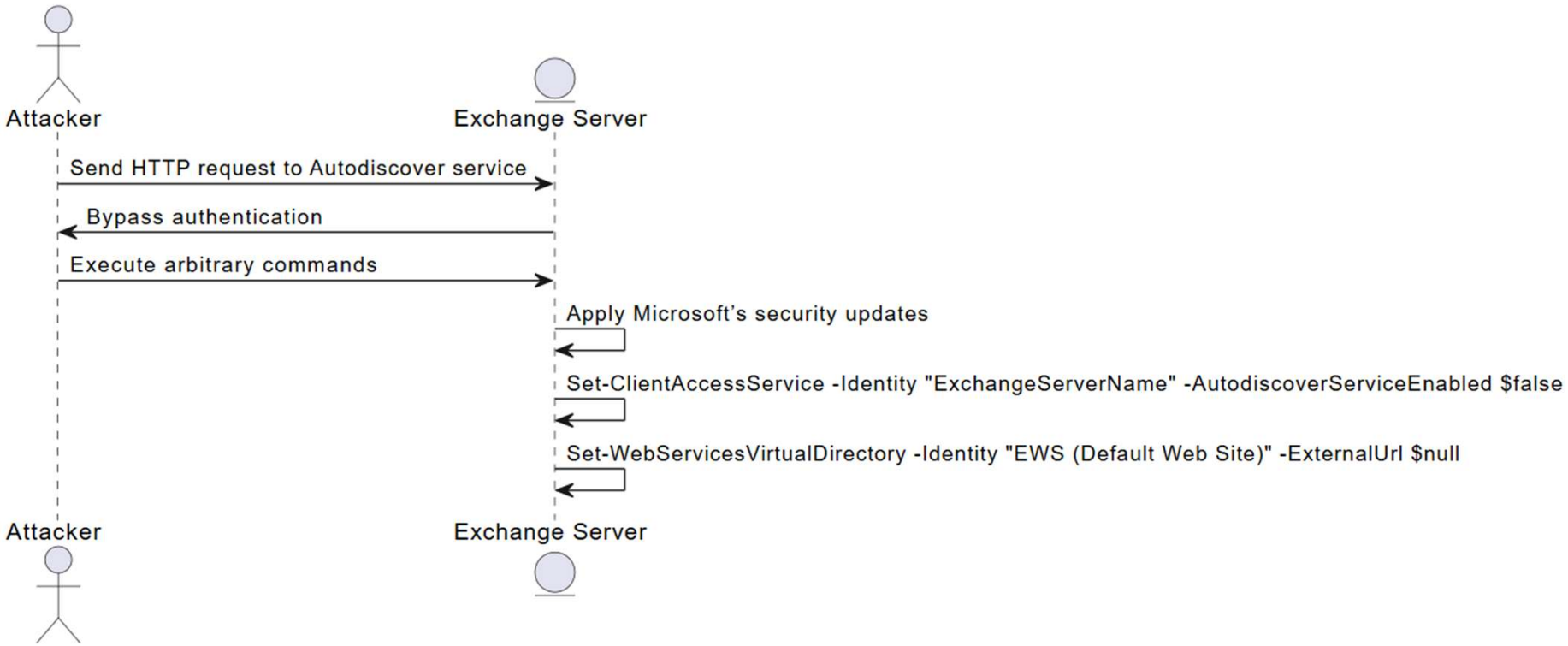
CTF Level : Medium to Hard

PREFACE

- **Critical Vulnerabilities :**

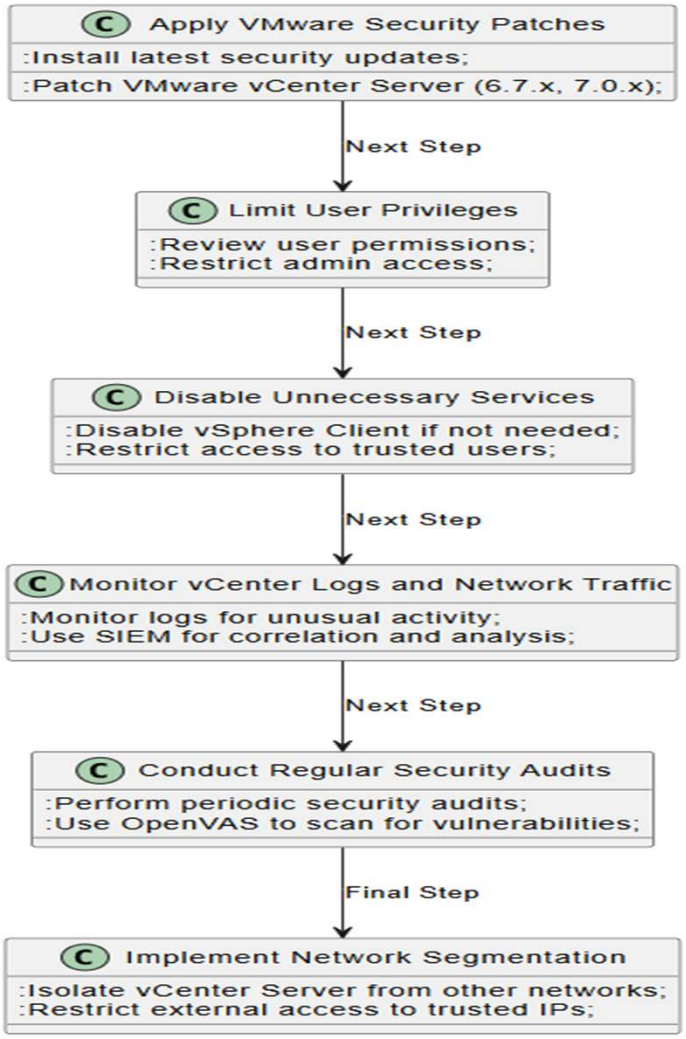
1. **CVE-2021-34473: ProxyShell (Microsoft Exchange) - Critical (CVSS 9.8)**
2. **CVE-2021-22972: VMware vCenter (vSphere) - Critical (CVSS 9.8)**
3. **CVE-2021-31207: DNS Cache Poisoning - Critical (CVSS 9.8)**
4. **CVE-2021-22005: VMware vCenter File Upload - Critical (CVSS 9.8)**
5. **CVE-2020-1472: Zerologon - Critical (CVSS 10.0)**
6. **CVE-2022-30190: Follina (Microsoft MSDT) - Critical (CVSS 7.8)**
7. **CVE-2022-0778: OpenSSL Infinite Loop - High (CVSS 9.1)**
8. **CVE-2021-34527: PrintNightmare - Critical (CVSS 8.8)**
9. CVE-2021-44228 (Log4Shell - Apache Log4j)

CVE-2021-34473: ProxyShell (Microsoft Exchange) - Critical (CVSS 9.8)



•**Apply Microsoft Security Patches**:
•Ensure the latest security updates from Microsoft are applied to affected Exchange Server versions (2013, 2016, 2019).
•Patches address vulnerabilities in the Autodiscover and EWS services.
•**Disable Autodiscover Service** (If not needed):
•Disable the Autodiscover service to reduce the attack surface.
•Use PowerShell to disable it if it's not required for your environment.
•**Restrict EWS Access**:
•Limit external access to **Exchange Web Services (EWS)** to trusted IPs only.
•Prevent unauthorized access by modifying the external URL to null.
•**Perform a Full Security Audit**:
•Conduct a security audit of the Exchange Server environment to identify other potential vulnerabilities.
•Use security scanning tools like **OpenVAS** for comprehensive assessments.
•**Monitor Logs and Network Traffic**:
•Continuously monitor Exchange logs and network traffic for suspicious activity.
•Use a **SIEM** tool to detect and correlate potential threats.
•**Regularly Update Security Measures**:
•Stay updated with the latest patches and security recommendations from Microsoft.
•Set up automatic updates where possible to ensure ongoing protection.
I

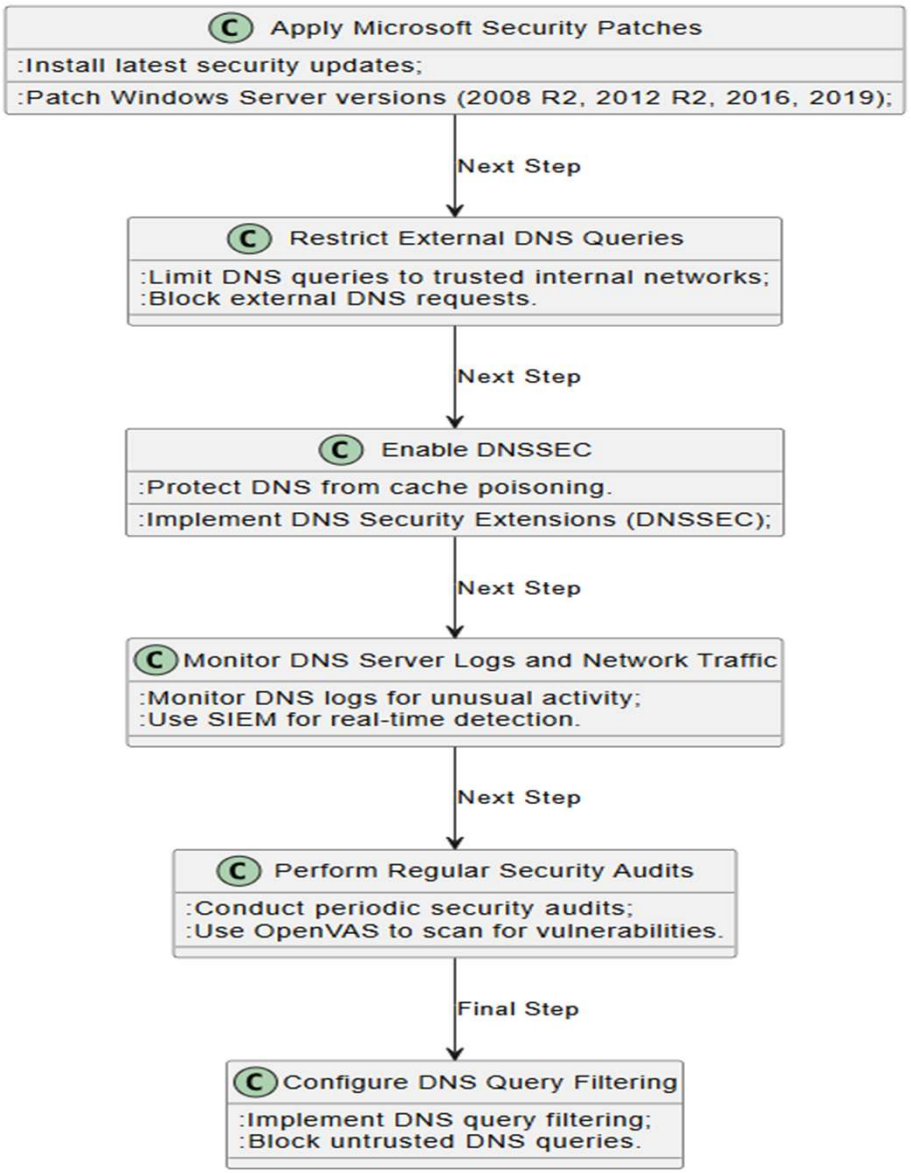
CVE-2021-22972: VMware vCenter (vSphere) - Critical (CVSS 9.8)



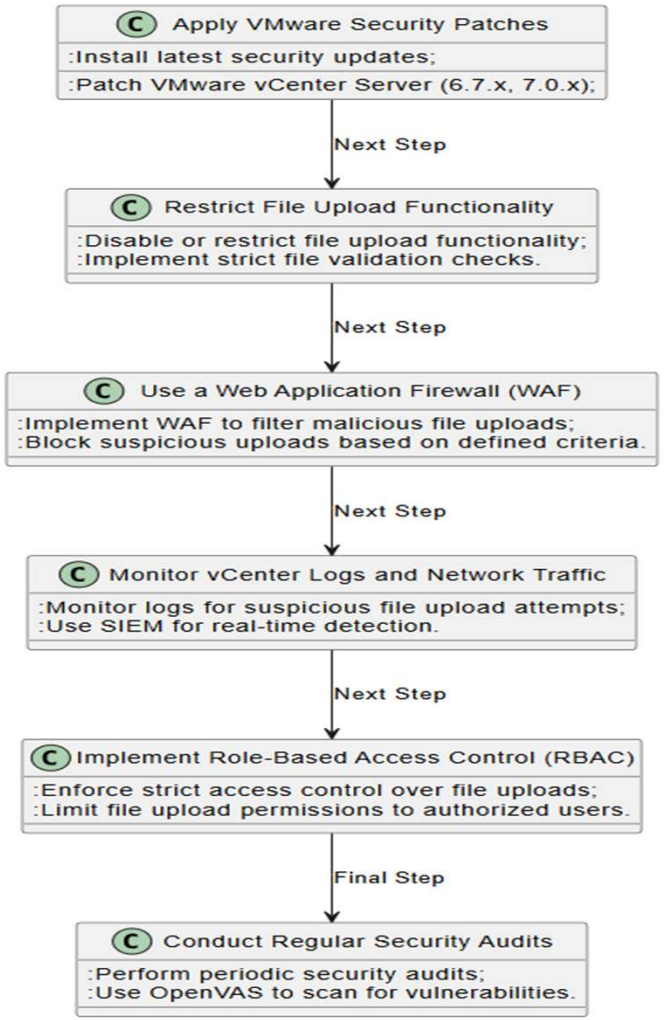
•**Apply VMware Security Patches**:
•Ensure that the latest security updates for VMware vCenter Server (6.7.x, 7.0.x) are installed.
•VMware has released patches to address this vulnerability and mitigate the risk of arbitrary command execution.
•**Limit User Privileges**:
•Ensure that only authorized users have elevated privileges within the vSphere Client.
•Review user permissions and restrict administrative access to minimize exposure to exploitation.
•**Disable Unnecessary Services**:
•Disable the **vSphere Client** if it is not required for your environment.
•Use the **vSphere Web Client** or other secure methods if needed, but restrict access to only trusted users.
•**Monitor vCenter Logs and Network Traffic**:
•Continuously monitor vCenter Server logs and network traffic for any unusual activity or failed login attempts.
•Implement a **SIEM** solution to correlate and analyze logs for potential threats.
•**Conduct Regular Security Audits**:
•Perform periodic security audits on the vCenter Server environment.
•Use security tools like **OpenVAS** to scan for vulnerabilities and ensure configurations are secure.
•**Implement Network Segmentation**:
•Isolate vCenter Server from other parts of the network, especially critical infrastructure.
•Restrict external access to the vCenter Server to trusted IPs only.

CVE-2021-31207: DNS Cache Poisoning - Critical (CVSS 9.8)

•**Apply Microsoft Security Patches**:
•Ensure the latest security updates from Microsoft for affected Windows Server versions
• (2008 R2, 2012 R2, 2016, 2019) are installed.
•Microsoft has released patches to fix the vulnerability in the DNS Server.
•**Restrict External DNS Queries**:
•Limit DNS query access to trusted internal networks only.
•Block or restrict external DNS requests to prevent malicious traffic from reaching the DNS server.
•**Enable DNSSEC (DNS Security Extensions)**:
•Implement DNS Security Extensions (DNSSEC) to protect the DNS server from cache poisoning.
•DNSSEC ensures that DNS responses are authenticated and tamper-proof.
•**Monitor DNS Server Logs and Network Traffic**:
•Continuously monitor DNS server logs for any unusual activity, such as unexpected DNS responses or failed
queries.
•Use **SIEM** tools to detect and correlate potential threats in real-time.
•**Perform Regular Security Audits**:
•Conduct periodic security audits to identify vulnerabilities and ensure DNS configurations are secure.
•Use security tools like **OpenVAS** to scan for DNS-related vulnerabilities.
•**Configure DNS Query Filtering**:
•Implement DNS query filtering to prevent the DNS server from accepting queries from untrusted sources.
•This can help block malicious requests before they are processed.

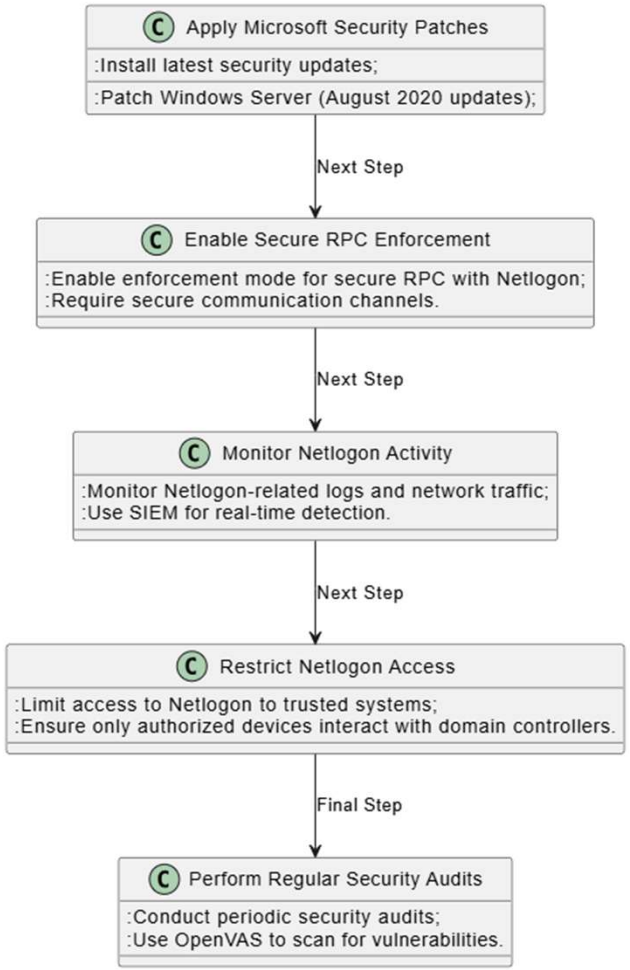

Apply Microsoft Security Patches
:Install latest security updates;
:Patch Windows Server versions (2008 R2, 2012 R2, 2016, 2019);
Next Step
Restrict External DNS Queries
:Limit DNS queries to trusted internal networks;
:Block external DNS requests.
Next Step
Enable DNSSEC
:Protect DNS from cache poisoning.
:Implement DNS Security Extensions (DNSSEC);
Next Step
Monitor DNS Server Logs and Network Traffic
:Monitor DNS logs for unusual activity;
:Use SIEM for real-time detection.
Next Step
Perform Regular Security Audits
:Conduct periodic security audits;
:Use OpenVAS to scan for vulnerabilities.
Final Step
Configure DNS Query Filtering
:Implement DNS query filtering;
:Block untrusted DNS queries.

CVE-2021-22005: VMware vCenter File Upload - Critical (CVSS 9.8)



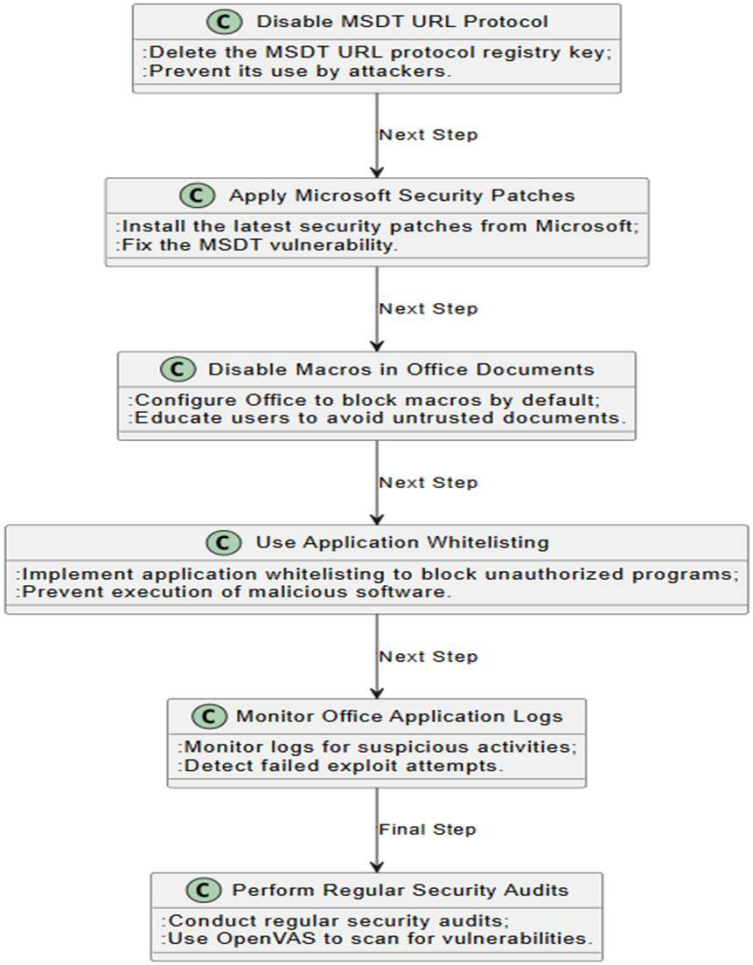
•**Apply VMware Security Patches**:
•Ensure that the latest security updates for VMware vCenter Server (6.7.x, 7.0.x) are installed.
•VMware has released patches that address the vulnerability and prevent unauthorized file uploads.
•**Restrict File Upload Functionality**:
•Disable or restrict the file upload functionality if it is not required for your environment.
•If file uploads are necessary, implement strict file validation checks to only allow safe file types.
•**Use a Web Application Firewall (WAF)**:
•Implement a **Web Application Firewall (WAF)** to filter and block malicious file uploads.
•A WAF can inspect HTTP requests and block any suspicious file uploads that do not meet the defined criteria.
•**Monitor vCenter Logs and Network Traffic**:
•Continuously monitor vCenter Server logs for any suspicious file upload attempts.
•Use **SIEM** tools to correlate and analyze logs for potential threats.
•**Implement Role-Based Access Control (RBAC)**:
•Ensure that only authorized users have permission to upload files to the vCenter Server.
•Implement **RBAC** to enforce strict access control over file upload functionality.
•**Conduct Regular Security Audits**:
•Perform periodic security audits on the vCenter Server environment to identify vulnerabilities and ensure that configurations are secure.
•Use tools like **OpenVAS** to scan for vulnerabilities related to file upload functionality.

CVE-2020-1472: Zerologon - Critical (CVSS 10.0)



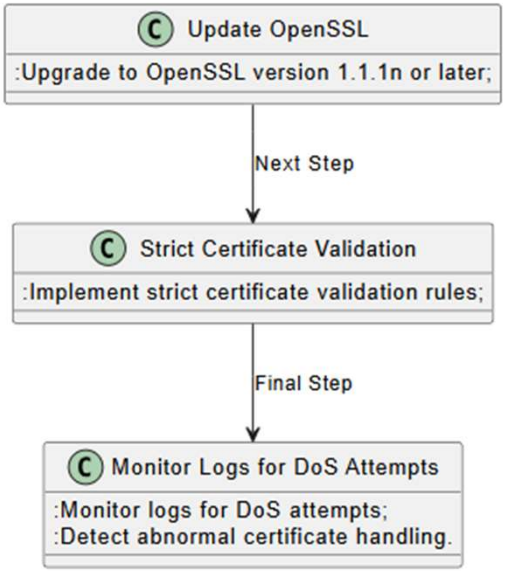
1. **Apply Microsoft Security Patches:**
    1. Ensure that the latest security updates for Windows Server (August 2020 updates) are installed.
    2. Microsoft released patches to fix the vulnerability in the Netlogon protocol.
2. **Enable Secure RPC Enforcement:**
    1. Enable enforcement mode for secure RPC with Netlogon to prevent unauthenticated access.
    2. This will require the use of secure communication channels for Netlogon authentication.
3. **Monitor Netlogon Activity:**
    1. Continuously monitor Netlogon-related logs and network traffic for suspicious activity.
    2. Use **SIEM** tools to detect and alert on any potential exploitation attempts.
4. **Restrict Netlogon Access:**
    1. Limit access to the Netlogon protocol to trusted internal systems only.
    2. Ensure that only authorized devices and users are able to interact with the domain controller.
5. **Perform Regular Security Audits:**
    1. Conduct periodic security audits to ensure that Netlogon configurations are secure.
    2. Use tools like **OpenVAS** to scan for vulnerabilities related to Netlogon.

CVE-2022-30190: Follina (Microsoft MSDT) - Critical (CVSS 7.8)



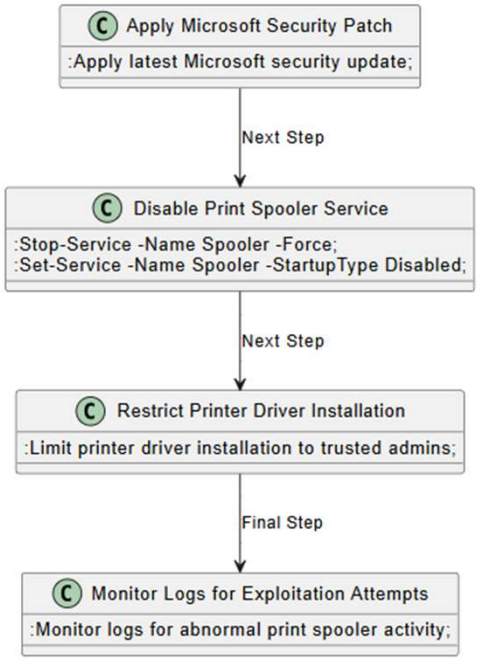
•**Disable MSDT URL Protocol**:
•Delete the MSDT URL protocol registry key to prevent its use by attackers.
•Run the following command to disable the protocol:
•**Apply Microsoft Security Patches**:
•Ensure that the latest security patches from Microsoft for the MSDT vulnerability are applied.
•Microsoft has released updates to address this issue in affected Windows versions.
•**Disable Macros in Office Documents**:
•Configure Microsoft Office to block or disable macros by default.
•Educate users to avoid opening untrusted Office documents that contain macros.
•**Use Application Whitelisting**:
•Implement application whitelisting to prevent the execution of unauthorized programs, especially those related to the MSDT exploit.
•**Monitor Office Application Logs**:
•Continuously monitor Office application logs for any suspicious activities or failed attempts to exploit the vulnerability.
•**Perform Regular Security Audits**:
•Conduct regular security audits to ensure that systems are protected against known vulnerabilities.
•Use security tools like **OpenVAS** to scan for potential weaknesses.

CVE-2022-0778 (OpenSSL Infinite Loop)



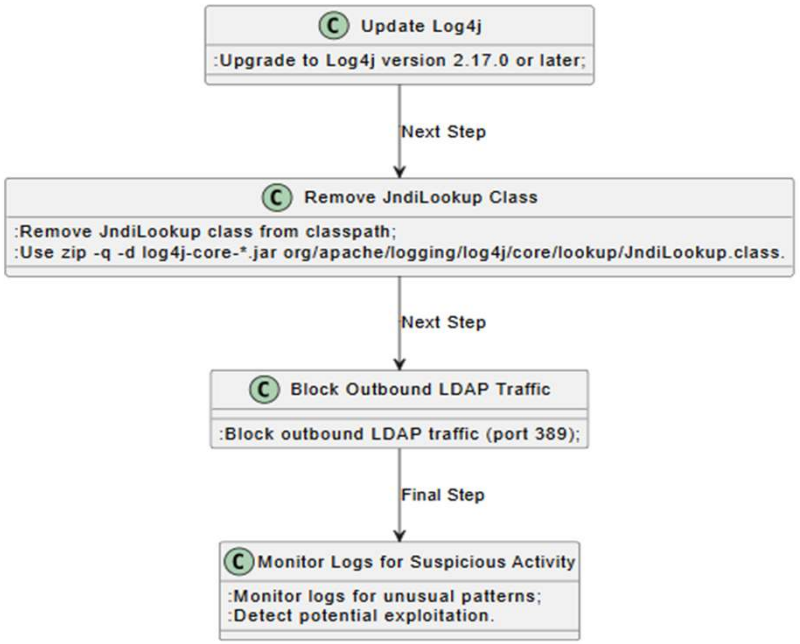
•**Update OpenSSL**:
•Upgrade to **OpenSSL version 1.1.1n or later** to address the infinite loop vulnerability.
•**Strict Certificate Validation**:
•Implement strict certificate validation rules to prevent the exploitation of malformed certificates.
•**Monitor Logs for Denial of Service Attempts**:
•Monitor system logs for any indications of denial of service (DoS) attempts or abnormal certificate handling.

CVE-2021-34527: PrintNightmare - Critical (CVSS 8.8)

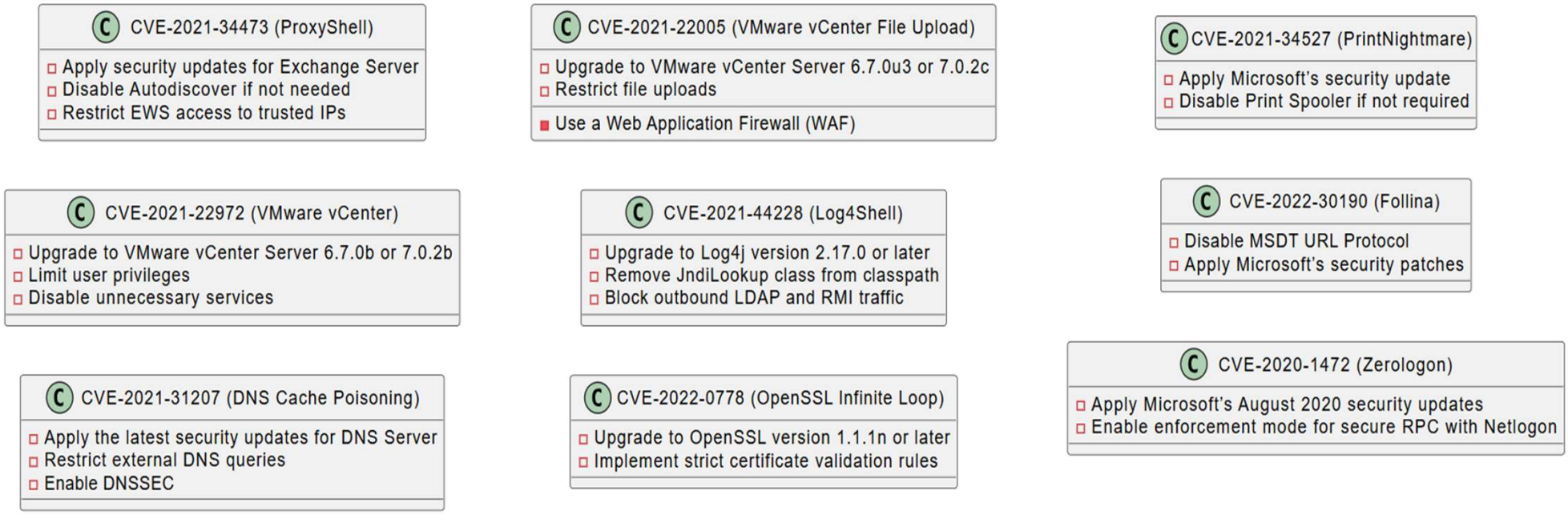


1. **Apply Microsoft Security Patch**:
   - Apply the latest **Microsoft security update** to patch the PrintNightmare vulnerability.
2. **Disable Print Spooler Service**:
   - If the print service is not required, disable the Print Spooler service using PowerShell:
3. **Restrict Printer Driver Installation**:
   - Limit who can install printer drivers to trusted administrators only.
4. **Monitor Logs for Exploitation Attempts**:
   - Continuously monitor system logs for signs of exploitation or abnormal print spooler activity.

CVE-2021-44228 (Log4Shell - Apache Log4j)



•**Update Log4j**:
•Upgrade to **Log4j version 2.17.0 or later** to resolve the vulnerability.
•**Remove JndiLookup Class**:
•Temporarily remove the **JndiLookup** class from the classpath using the following command:
•**Block Outbound LDAP Traffic**:
•Block outbound LDAP traffic (port 389) at the firewall level to prevent exploitation of the vulnerability.
•**Monitor Logs for Suspicious Activity**:
•Continuously monitor logs for unusual patterns that may indicate exploitation attempts.


CVE-2021-34473 (ProxyShell)
Apply security updates for Exchange Server
Disable Autodiscover if not needed
Restrict EWS access to trusted IPs
CVE-2021-22005 (VMware vCenter File Upload)
Upgrade to VMware vCenter Server 6.7.0u3 or 7.0.2c
Restrict file uploads
Use a Web Application Firewall (WAF)
CVE-2021-34527 (PrintNightmare)
Apply Microsoft's security update
Disable Print Spooler if not required
CVE-2021-22972 (VMware vCenter)
Upgrade to VMware vCenter Server 6.7.0b or 7.0.2b
Limit user privileges
Disable unnecessary services
CVE-2021-44228 (Log4Shell)
Upgrade to Log4j version 2.17.0 or later
Remove JndiLookup class from classpath
Block outbound LDAP and RMI traffic
CVE-2022-30190 (Follina)
Disable MSDT URL Protocol
Apply Microsoft's security patches
CVE-2021-31207 (DNS Cache Poisoning)
Apply the latest security updates for DNS Server
Restrict external DNS queries
Enable DNSSEC
CVE-2022-0778 (OpenSSL Infinite Loop)
Upgrade to OpenSSL version 1.1.1n or later
Implement strict certificate validation rules
CVE-2020-1472 (Zerologon)
Apply Microsoft's August 2020 security updates
Enable enforcement mode for secure RPC with Netlogon