Phase 4. Threat Assessment

Goal: Create a hypothetical threat assessment based on vulnerabilities you expect to find when you perform your actual scans against the client's network.

Procedure: Assume the scenarios below are what you are most likely to encounter when you begin your actual work.

Scenario 1: Unpatched RDP is exposed to the internet

- **Description of the vulnerability**

RDP is a network protocol that allows a person to remotely control a computer that is attached to the internet. The remote person sees whatever is on the screen of the computer they are controlling and their keyboard and mouse act just like the ones physically attached to the remote computer. For a remote desktop connection to be established, the local and remote machines need to authenticate via a username and password. Cyber actors can infiltrate the connection between the machines and inject malware or ransomware into the remote system. Attacks using the RDP protocol do not require user input, making intrusions difficult to detect.

- **Operating systems/versions affected**

Windows 2000, Windows Vista, Windows XP, Windows 7, Windows Server 2003, Windows Server 2003 R2, WIndows Server 2008, WIndows Server 2008 R2, Windows 10, Windows 11, Apple macOS

- **Risks of attempting to exploit** (e.g., might crash the host or lock out an account)

An attacker with a machine-in-the-middle (MitM) position who successfully exploited this vulnerability could compromise the confidentiality and integrity of data when the targeted user connects to a trusted server. Once a hacker finds an accessible system, they will do one of two things and sometimes both. First, they may exploit the system themselves. The other option is to sell the stolen RDP login credentials on the Dark Web. The Dark Web is a portion of the internet that is only accessible when using a Tor browser, this area is where most of the criminal activity on the internet is monetized. The value of the credentials is based on the location of the compromised system, and what the system has access to. The possible threats from someone accessing a computer on your network via RDP include data and financial theft. Malware and ransomware can be installed and activated to send infected e-mails to your contacts, vendors or customers.

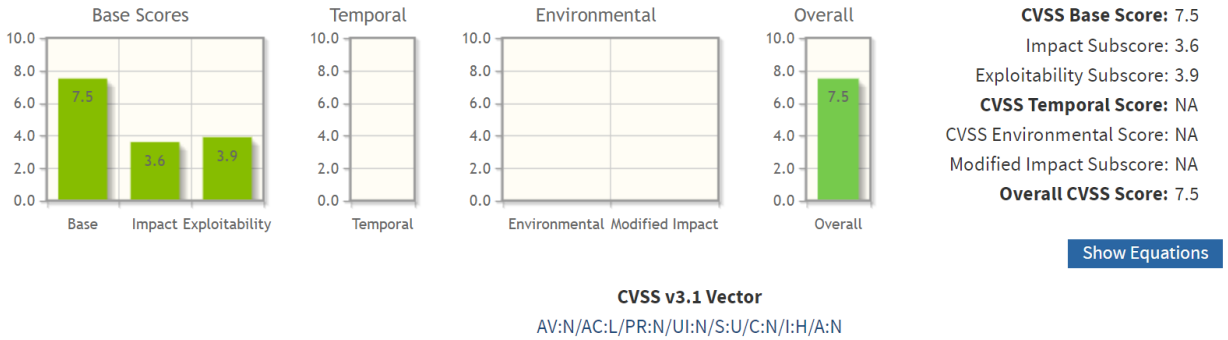
- **Risk (what could you or a threat actor do upon successful exploitation)?**

1. An attacker may take control of a user's device or gain a foothold in the system to maintain persistent remote access.

2. Malicious code that autonomously replicates itself to other devices on the same network and these vulnerabilities can put the whole enterprise network at risk.
3. Harvesting credentials
4. Malicious code
5. Brute-force password guessing
6. Identify weak passwords
7. Discover unsecured ports
8. Outdated software

- **Remediation action**
    1. Use group policies to specify application allow lists and block lists
    2. Use the regedit tool to prevent the built-in Windows Help feature from being opened
    3. If not using RDP, close TCP port 3389 on the computers and routers
    4. Make sure all security patches have been located on your computers
    5. Make sure all security patches have been loaded
    6. Use 2MFA authentication
    7. Enable event logging and review logs on a regular, at least weekly, basis
    8. Never have RDP active on a critical network device, such as a server
    9. Use VPN connections whenever possible to encrypt RDP traffic
    10. Make sure any public cloud-based systems are not using RDP
    11. Implement Network Level Authentication
    12. Implement an RDP Gateway
    13. Enable RBAC restrictions
    14. Enable Automatic Updates

- **CVSS score**



Scenario 2: Web application is vulnerable to SQL Injection

- **Description of the vulnerability**

When a cybercriminal inserts a malicious SQL injection, a line of code is added that can interfere with the queries the application itself makes sends to its database. By

doing this, the database can be exploited in a way that allows the threat actor to view data that they would otherwise not have access to.

- **Operating systems/versions affected**

Windows, Kali Linux, MacOS - Any platform that requires interaction with a SQL database.

- **Risks of attempting to exploit (e.g., might crash the host or lock out an account)**

A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system. SQL injection attacks are a type of injection attack, in which SQL commands are injected into data-plane input in order to affect the execution of predefined SQL commands.

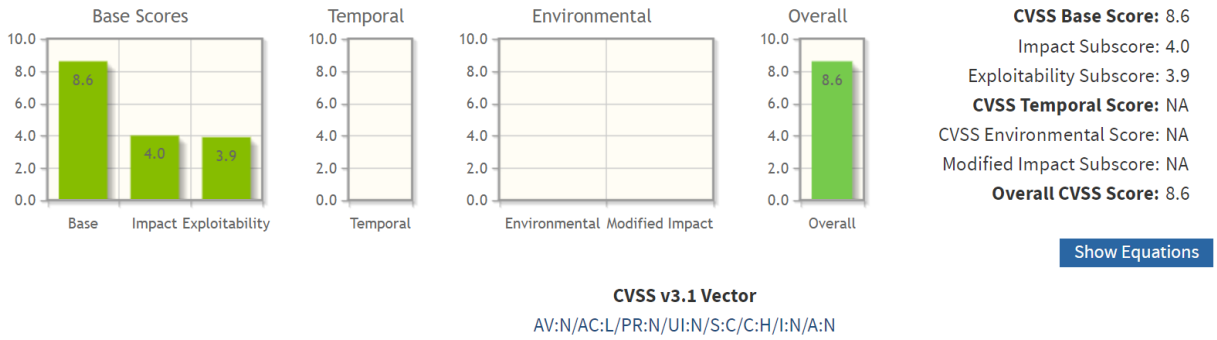
- **Risk (what could you or a threat actor do upon successful exploitation)?**

1. Using SQL injection, attackers can retrieve and alter data, which risks explaining sensitive company data.
2. Depending on the data stored on the SQL server, an attack can expose private user data, such as credit numbers.
3. Bypassing Authentication
4. Install malicious code
5. Identifying Injectable Parameters
6. Executing Remote Commands
7. Denial of Service
8. Database Fingerprinting
9. Spoof identity
10. Cause repudiation issues (such as voiding transactions or changing balances)
11. Destroy the data or make it otherwise unavailable
12. Execute administration operations on the DB.

- **Remediation action**

1. Train and maintain awareness
2. Use whitelists
3. Use least privilege
4. Sanitize the Data / Input validation
5. Escaping All User Supplied Input
6. Use of Prepared Statements (with Parameterized Queries)
7. Input validation

● **CVSS score**



Scenario 3: Default password on Cisco admin portal

● **Description of the vulnerability**

If you leave your default password unchanged and use it repeatedly, you put your device and data at risk. An intact passcode provides opportunistic hackers with an attack vector to gain unwarranted access to your device and data. This problem escalates If the device is connected to a corporate network, spreading that security risk throughout the corporation.

● **Operating systems/versions affected**

Cisco switch, router, firewall, administrative web application, database, endpoints

● **Risks of attempting to exploit (e.g., might crash the host or lock out an account)**

A default password is a pre-configured passcode for a device to initiate its first setup. Common default passwords include “**admin**”, “**password**”, “**guest**”, or the brand name such as “**Cisco**”. Companies typically use a single default passcode for the same model or batch of products. It can usually be found on their official website or through their given manuals, not to mention dozens of websites that publish compiled lists of default login credentials categorized by brand, product, and model. So, a single default password is the default configuration for numerous machines.

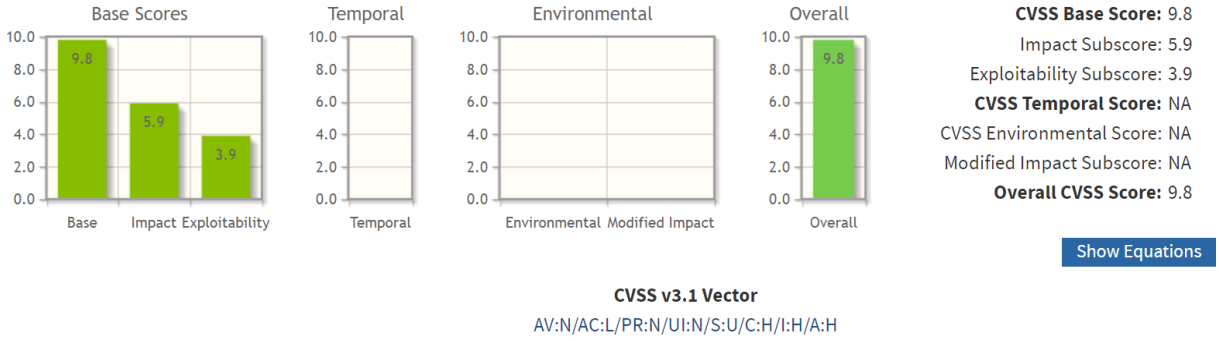
● **Risk (what could you or a threat actor do upon successful exploitation)?**

1. An attacker could use this knowledge to authenticate with administrative privileges and arbitrarily change the configuration of Cisco Network Registrar
2. Attackers can easily obtain default passwords and identify internet-connected target systems. Passwords can be found in product documentation and compiled lists available on the internet. It is possible to identify exposed systems using search engines like Shodan.
3. An attacker with knowledge of the password and network access to a system can log in, usually with root or administrative privileges. Further consequences depend on the type and use of the compromised system.

● **Remediation action**

Default passwords are nothing more than, hence should be treated as, placeholders. They should only be used for the first setup or just after a factory reset of your device. Users are typically prompted to change the default password after entering it for the first time. Some companies enforce a change of default password upon first use, such that the setup process cannot proceed otherwise. However, the safest and easiest way to get around this issue is to change it using a good password manager.

● **CVSS score**



Scenario 4: Apache web server vulnerable to CVE-2019-0211

● **Description of the vulnerability**

Lets an attacker execute unprivileged scripts, usually run by Apache with lowered privileges to take over the main Apache process. This can also lead to an attacker gaining root access to the server by simply running a script.

● **Operating systems/versions affected**

This vulnerability affects Apache web server releases for Unix systems, from version 2.4.17 (Oct. 9, 2015) to version 2.4.38 (Apr. 1, 2019)

● **Risks of attempting to exploit (e.g., might crash the host or lock out an account)**

Might crash the host or lock out an account

● **Risk (what could you or a threat actor do upon successful exploitation)?**

CVE-2019-0211 vulnerability poses severe risks when the web server is used for running shared hosting instances, in this scenario, users with limited permissions could exploit the flaw to get root privileges, allow them to gain complete control of the machine,

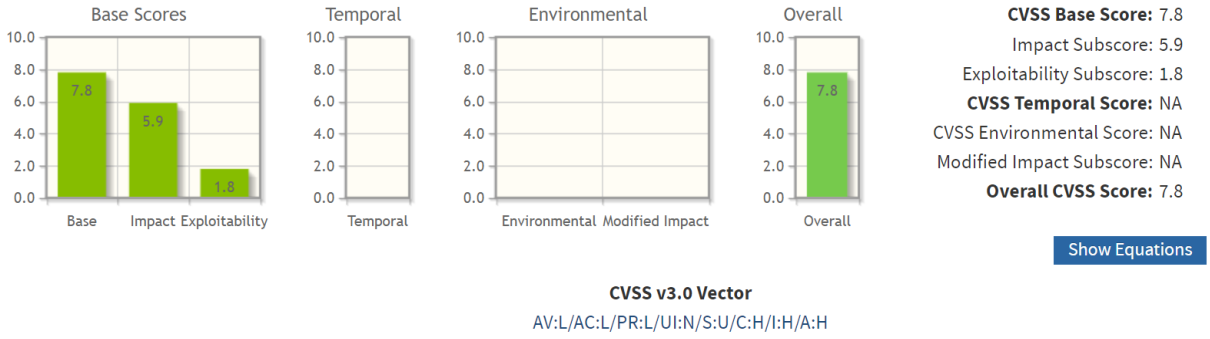
using scripts and run commands on vulnerable Apache web servers. It is very common to give unprivileged users the ability to write their own scripts.

● **Remediation action**

System administrators can patch the flaw by updating their servers to Apache httpd version 2.4.39. Developers, programmers, and system admins that use Apache should also employ the principle of least privilege to prevent threats that may exploit related vulnerabilities.
Safeguards:

1. network access to only trusted users,
2. and employing IP-based access control lists (ACLs) to allow only trusted systems to access the affected systems.

● **CVSS score**



Scenario 5: Web server is exposing sensitive data

● **Description of the vulnerability**

Sensitive data exposure occurs as a result of not adequately protecting a server where information is stored. This might be a result of a multitude of things such as weak encryption, no encryption, software flaws, or when someone mistakenly uploads data to an incorrect database.

● **Operating systems/versions affected**

Any application running a web server that has the vulnerability

● **Risks of attempting to exploit (e.g., might crash the host or lock out an account)**

Might crash the host or lock out an account.

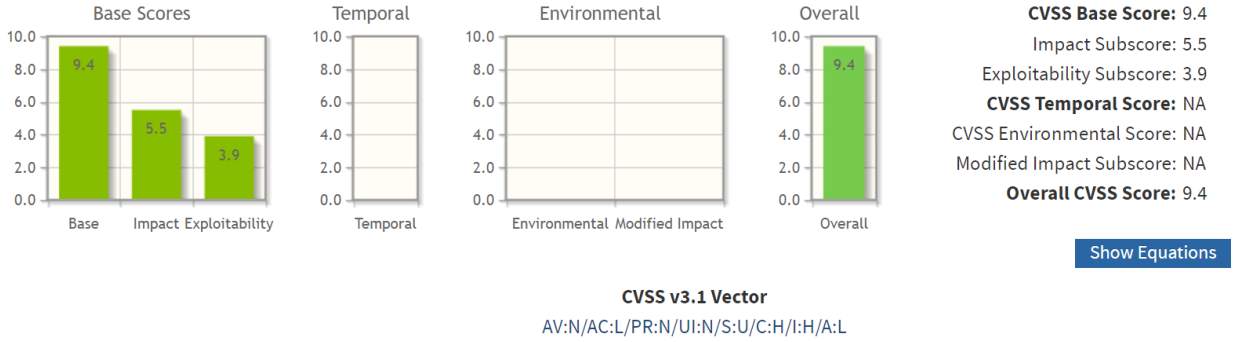
● **Risk (what could you or a threat actor do upon successful exploitation)?**

Sensitive data is any information that is meant to be protected from unauthorized access. Sensitive data exposure occurs as a result of not adequately protecting a database where information is stored. This might be a result of a multitude of things such as weak encryption, no encryption, software flaws, or when someone mistakenly uploads data to an incorrect database. Different types of data can be exposed in a sensitive data exposure. Banking account numbers, credit card numbers, healthcare data, session tokens, Social Security number, home address, phone numbers, dates of birth, and user account information such as usernames and passwords are some of the types of information that can be left exposed.

● **Remediation action**

1. Use SSL
2. Use HTTPS security
3. Use strong cryptographic algorithms or keys
4. Using salt with passwords
5. Encryption All Sensitive Data
6. Classifying Data
7. Use Security Testing Tools
8. Don't hold on to Sensitive Data

● **CVSS score**



Scenario 6: Web application has broken access control

● **Description of the vulnerability**

Broken access control vulnerability is a type of security flaw that allows an unauthorized user access to restricted resources.

● **Operating systems/versions affected**

Any application running a web server that has the vulnerability

● **Risks of attempting to exploit (e.g., might crash the host or lock out an account)**

Might crash the host or lock out an account

● **Risk (what could you or a threat actor do upon successful exploitation)?**

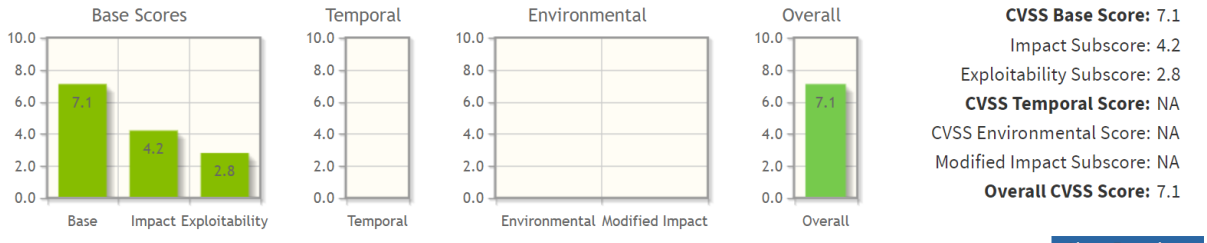
If an attacker is able to gain access to sensitive data, they may be able to use this information for malicious purposes, such as identity theft or fraud. Additionally, data breaches can damage an organization's reputation and lead to financial losses. Organizations subject to regulatory requirements, such as HIPAA or PCI DSS, must ensure access controls comply with these regulations. If an organization's access controls aren't up to par, they may be subject to fines or other penalties. Finally, broken access controls can also lead to operational disruptions. When attackers can gain access to critical systems, they may be able to disable or damage them, leading to significant downtime and financial loss. More risks include: 1. Exposure to Unauthorized Content, 2. Privilege Escalation, and 3. Distributed Denial of Service.

● **Remediation action**

There are many different access control systems, but they all have the same goal: to keep unauthorized people from entering an area or using a resource.

1. Enforce Record Ownership
2. Enable RBAC
3. Constant Testing and Auditing of Access Controls
4. Deny by Default

● **CVSS score**



Scenario 7: Oracle WebLogic Server vulnerable to CVE-2020-14882

● **Description of the vulnerability**

Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. (Confidentiality, Integrity and Availability impacts).

● **Operating systems/versions affected**

Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0.

● **Risks of attempting to exploit (e.g., might crash the host or lock out an account)**

Might crash the host or lock out an account

● **Risk (what could you or a threat actor do upon successful exploitation)?**

CVE-2020-14882 is a critical remote code execution vulnerability in Oracle WebLogic Server. It allows unauthenticated attackers to take full control of vulnerable systems, posing risks such as data theft, malware installation, and operational disruption.

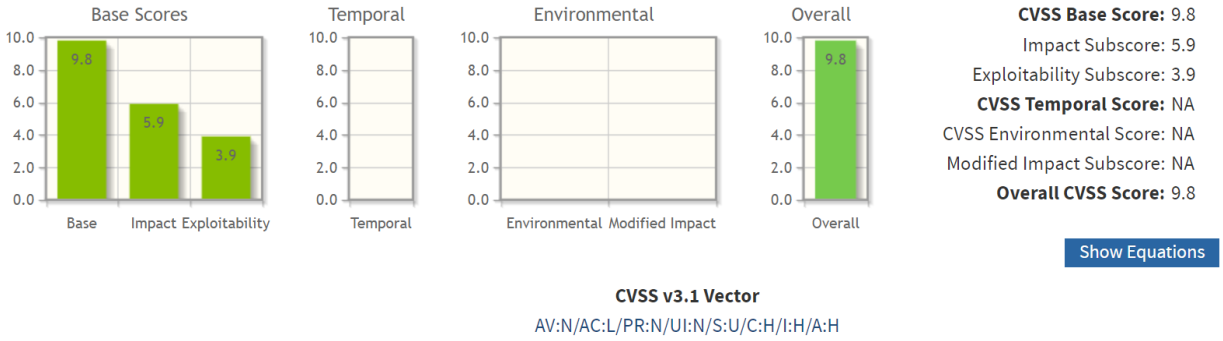
● **Remediation action**

Oracle strongly recommends that customers apply the updates provided by this Security Alert as soon as possible after applying the October 2020 Critical Patch Update. If immediate patching is impossible,

These mitigations include temporarily:

- Removing the admin portal from the public internet
- reviewing application logs for HTTP requests that include the double-encoded path traversal *%252E%252E%252F* and the admin portal *console.portal* in the request URI
- Monitoring network traffic for suspicious HTTP requests (if possible)
- Monitoring for any suspicious processes created by the application

● **CVSS score**



Scenario 8: Misconfigured cloud storage (AWS security group misconfiguration, lack of access restrictions)

● **Description of the vulnerability**

Cloud misconfiguration refers to any glitches, gaps, or errors that could expose your environment to risk during cloud adoption.

● **Operating systems/versions affected**

Any cloud storage that contains a misconfiguration

● **Risks of attempting to exploit (e.g., might crash the host or lock out an account)**

Might crash the host or lock out an account

● **Risk (what could you or a threat actor do upon successful exploitation)?**

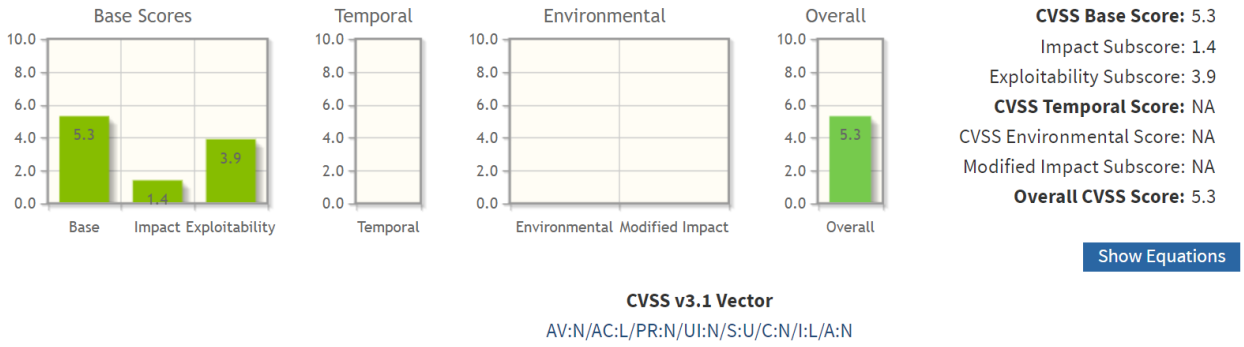
These cyber threats come in the form of security breaches, external hackers, ransomware, malware, or insider threats that use vulnerabilities to access your network. Cloud misconfigurations result in companies exposing unencrypted or sensitive data to the public internet. This results in data leakage and downtime, which could lead to serious reputational damage and financial loss for the companies or government entities.

● **Remediation action**

1. Implement logging practices
2. Enable encryption
3. The rule of Least Privilege
4. Perform consistent misconfiguration audits
5. Create, apply, and communicate strong security policies

6. Implement an automated remediation solution to monitor and alert for misconfiguration issues

- **CVSS score**



Scenario 9: Microsoft Exchange Server vulnerable to CVE-2021-26855

- **Description of the vulnerability**

This is a server-side request forgery (SSRF) vulnerability in Exchange which allows the attacker to send arbitrary HTTP requests and authenticate as the Exchange Server.

- **Operating systems/versions affected**

- Microsoft Exchange Server 2013
- Microsoft Exchange Server 2016
- Microsoft Exchange Server 2019

- **Risks of attempting to exploit (e.g., might crash the host or lock out an account)**

Might crash the host or lock out an account

- **Risk (what could you or a threat actor do upon successful exploitation)?**

This flaw enabled attackers to bypass authentication and execute arbitrary code with high privileges on vulnerable Exchange Servers. ProxyLogon allowed attackers to abuse the server-side request forgery (SSRF) technique to send crafted requests to the Exchange Control Panel (ECP) and gain unauthorized access. By exploiting this

vulnerability chain, threat actors could achieve remote code execution and potentially compromise the entire Exchange Server environment.

1. Authentication Bypass: ProxyLogon bypassed authentication mechanisms, granting attackers direct access to Exchange Server resources without needing valid credentials. This was achieved by sending specially crafted requests to the ECP.
2. Remote Code Execution: Once authenticated, attackers could execute arbitrary code on the Exchange Server, potentially leading to data exfiltration, further network compromise, or installation of persistent backdoors.

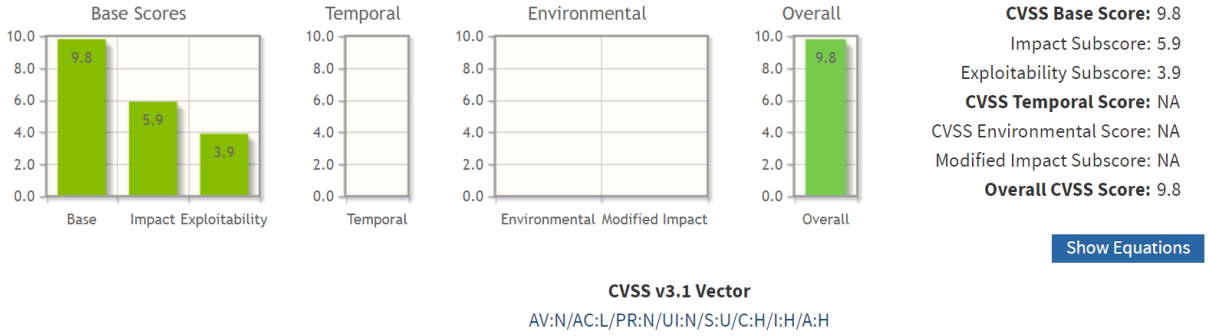
IMPACT

1. Data Theft: Successful exploitation of ProxyLogon could lead to unauthorized access to sensitive data stored within Exchange Server mailboxes. Attackers could exfiltrate emails, contacts, attachments, and other confidential information, potentially compromising the organization's intellectual property or customer data.
2. System Compromise: By executing arbitrary code on the Exchange Server, threat actors could gain control over the entire environment. This enabled them to pivot to other systems, escalate privileges, or launch additional attacks within the organization's network.
3. Further Exploitation: ProxyLogon served as an initial foothold for subsequent attacks. Once inside the network, threat actors could move laterally, exploit other vulnerabilities, or deploy ransomware to disrupt operations or demand hefty extortion payments.

- **Remediation action**

1. Patching: Applying the available security updates and patches provided by Microsoft is critical to remediate ProxyLogon and protect Exchange Server environments from potential exploitation. This should be done immediately to prevent unauthorized access.
2. Incident Response: Organizations must initiate an incident response plan to identify any signs of compromise, investigate the extent of the breach, and contain the impact. This includes conducting thorough system audits, monitoring network traffic, and analyzing log data to detect any unauthorized activities.
3. Enhanced Monitoring: Implementing robust network monitoring and intrusion detection systems can help identify and respond to any suspicious activities related to ProxyLogon or potential follow-up attacks.
4. User Awareness and Training: Educating users about the risks of phishing attacks, suspicious emails, and social engineering techniques helps mitigate the likelihood of falling victim to such attacks. Users should be vigilant and report any unusual or suspicious emails or activities to the appropriate security teams.

- **CVSS score**



Course content reference: You may need to refer back to the unit on risk assessment to analyse the vulnerabilities and assess what threat they pose to Artemis. In addition, review the two videos: Vulnerability Management: Assessing the Risks with CVSS v3.1 and Implementing the NIST Risk Management Framework in the Audit and Risk Management subunit. Remember: The threat depends on the likelihood and impact of the vulnerabilities being exploited and requires a review and knowledge of the current threats.

Include all the information and risk ratings to determine the threat profile for Artemis.

Time estimate: 6 hours

REFERENCES

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-35332
https://www.dnv.com/article/hackers-are-exploiting-remote-desktop-protocol-rdp--134501
https://www.geeksforgeeks.org/risks-associated-with-sql-injection/
https://www.makeuseof.com/what-is-sql-injection/
https://owasp.org/www-community/attacks/SQL_Injection
https://passwarden.com/help/use-cases/cisco-default-password
https://www.cisa.gov/news-events/alerts/2013/06/24/risks-default-passwords-internet
https://cloudsek.com/threatintelligence/carpe-diem-cve-2019-0211-apache-local-privilege-escalation#:~:text=This%20vulnerability%20was%20a%20critical,by%20simply%20running%20a%20script.
https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/cve-2019-0211-patched-apache-http-server-root-privilege-escalation-flaw-a-priority-for-web-hosting-providers
https://securityaffairs.com/83225/hacking/cve-2019-0211-apache-flaw-allows-getting-root-access-via-script.html
https://www.contrastsecurity.com/glossary/sensitive-data-exposure
https://us.norton.com/blog/privacy/sensitive-data-exposure-how-its-different-from-data-breach
https://medium.com/analytics-vidhya/how-to-prevent-sensitive-data-exposure-owasp-top-10-fd05550e0ac2
https://gaya3-r.medium.com/sensitive-data-exposure-19ac6e3090f4
https://www.eccouncil.org/cybersecurity-exchange/web-application-hacking/broken-access-control-vulnerability/
https://docs.google.com/document/d/17RGNt9hD6IzgOivdE-H1pjyqWbU0Pp6VP6XQERulqRg/edit
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14882#:~:text=Easily%20exploitable%20vulnerability%20allows%20unauthenticated,%2C%20Integrity%20and%20Availability%20impacts).

https://yoroi.company/research/cve-advisory-full-disclosure-cisco-ise-broken-access-control/
https://www.secpod.com/blog/oracle-emergency-fix-for-critical-rce-flaw-in-weblogic-server-cve-2020-14750/

https://blog.invgate.com/patch-cve-2020-14882#:~:text=CVE%2D2020%2D14882%20is%20a%20critical%20remote%20code%20execution%20vulnerability.malware%20installation%2C%20and%20operational%20disruption.
https://www.barradvisory.com/blog/cloud-misconfiguration/
https://www.upguard.com/blog/cve-2021-26855
https://cybersoochna.com/cve-2021-26855-proxylogon-zero-day-vulnerability-in-microsoft-exchange-server/