Detailed Technical Report:

Capstone Project

By:

Daniel Durjan

Table of Contents

Scope of Work

- The Scope of work is all of Artemis, Incorporated (“Artemis”) and its various IT, IT Security, and IT audit work-related products, processes, services, and entities (i.e., human elements). Our scope will allow us to perform reconnaissance of the client and its entities, run target identification against entities, run vulnerability scans against the external network, analysis of (notional, yet specific) scenarios and their remediation.

Project Objectives

- Conduct a thorough analysis of Artemis, Incorporated (“Artemis”) and its various IT, IT Security, and IT audit work-related products, processes, services, and entities (i.e., human elements).

- Identify insecurities and vulnerabilities as well as offer tools to mitigate/patch/remediate those failings.

- Assess the threats and make recommendations.

- Penetration Testing, specifically, will lead to better, safer, and more secure products, processes, services, and entities.

    - Entries will follow the format

Risk name

    - Fixing this will prevent the risk of ________.

    - This will be more aligned with the Information Security objective ______.

- This results in better achieving the organization’s objective ________

1) Scenario 1: Unpatched RDP is exposed to the internet

a. Fixing this will prevent the risk of "Rogue Sessions, Hijacking, Inappropriate access, exploits opportunity, Privileged escalation, HUGE opportunity for social engineering, Insecure management which leads to password cracking.

b. "This will be more aligned with the Information Security objective Secure Server.

c. This results in better achieving the organization’s objective Information being confidential and being available.

2) Scenario 2: Web application is vulnerable to SQL Injection

a. Fixing this will prevent the risk of ".Get other people's credentials --> privilege escalation, Complete access to all data --> ransom(ware), Potential access to the Operating System = VERY BAD "

b. This will be more aligned with the Information Security objective of Secure Web Application.

c. This results in better achieving the organization’s objective of having a Web program that is safe and secure for customer information.

3) Scenario 3: Default password on Cisco admin portal (Assuming router)

a. Fixing this will prevent the risk of major security risk for that device, and personal network. In this case, a major security hole in a business. May leak to other parts of the network leading to privilege escalation.

b. This will be more aligned with the Information Security objective of Secure Network Devices.

c. This results in better achieving the organization’s objective Securing Equipment.

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

a. Fixing this will prevent the risk of Privilege escalation, full access to a server, and full control over database

b. This will be more aligned with the Information Security objective Secure Servers

c. This results in better achieving the organization’s objective Appropriate employee/customer access.

5) Scenario 5: Web server is exposing sensitive data

a. Fixing this will prevent the risk of the web application going down in terms of service degradation, parts of the database can be accidentally overwritten, and triggering automatic responses. It could also result in a massive data breach leading to Identity Theft

b. This will be more aligned with the Information Security objective Preventing Breaches

c. This results in better achieving the organization’s objective protecting customer information.

6) Scenario 6: Web application has broken access control

a. Fixing this will prevent the risk of Privilege escalation, distributed Denial of Service (which comes from having control over multiple accounts)

b. This will be more aligned with the Information Security objective Appropriate Authority for Users.

c. This results in better achieving the organization’s objective safer/more secure product offering to customers/potential attackers.

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

a. Fixing this will prevent the risk of crashing server, corrupting data, server being taken over, loss of confidentiality.

b. This will be more aligned with the Information Security objective Data Security.

c. This results in better achieving the organization’s objective Protect Customer Information

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

a. Fixing this will prevent the risk of stealing personal data/digital skimming.

b. This will be more aligned with the Information Security objective Proper Configuration

c. This results in better achieving the organization's objective Protect Customer Information

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

a. Fixing this will prevent the risk of redirecting **our** users to other pages and user impersonation.

b. This will be more aligned with the Information Security objective Keep Patches up to Date.

c. This results in better achieving the organization's objective Secure Equipment and protect users from potential threats.

Assumptions

- We assume that all testers are competent and trigger potential dangers while conducting penetration testing.
    - However, this entire process can still be dangerous. It is imperative that testers find the appropriate times to test to minimize technology going down, temporarily or permanently, and disrupting business operations.
    - E.g., we'd assume that a penetration tester is unlikely to corrupt data on a webserver while trying to pen-test that server during **peak** business hours.

Timeline

- The Penetration Test will start July 1, 2022 and end December 1, 2022.

- This period will focus extensively on Artemis.

- The Tester will not be held accountable for potential mistakes/errors/damage that occur as a result of pen-testing but will take every reasonable precaution before testing. This will include providing an outline of what may be potentially risky.

Summary of Findings

Overall, Artemis is not in a bad position. There were 9 major vulnerabilities that we found. While it is our recommendation that these risks be remediated, that does not call for total panic.

Recommendations

For this section, the format will follow as such:

x) Risk name

a. This can be remediated by: _____.

1) Scenario 1: Unpatched RDP is exposed to the internet

a. This can be remediated by: Access Lists with just-in-time access, Full monitoring, High Encryption, Session Management (because having orphan sessions can be bad)

2) Scenario 2: Web application is vulnerable to SQL Injection

a. This can be remediated by: Input Validation, parametrized queries e.g., prepared statements, turning of ability to see database errors leading to errors give away info

3) Scenario 3: Default password on Cisco admin portal (Assuming router)

a. This can be remediated by: Using a good password manager or simply changing it immediately

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

a. This can be remediated by: Updating to version 2.4.39

5) Scenario 5: Web server is exposing sensitive data

a. This can be remediated by: Using programs that scan for potentially sensitive information and alerting staff, by auditing files, and by cataloging/categorizing data effectively.

6) Scenario 6: Web application has broken access control

a. This can be remediated by: implementing Deny by Default principle, mandating Continuous Auditing, better Logs, and using a Rate Limit API

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

a. This can be remediated by: installing the most update patch.

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

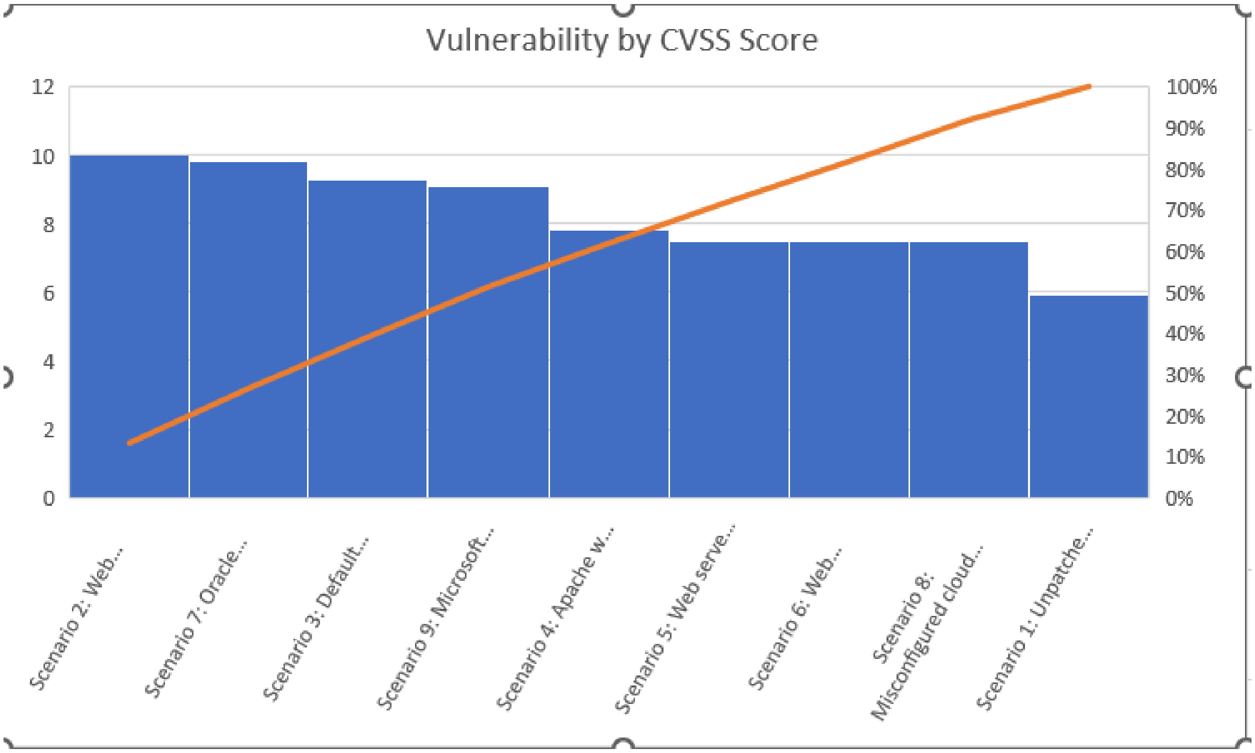
    a. This can be remediated by: implementing better logging practices, using Encryption, CHECKING PERMISSIONS across the board, Carefully considering security policies and priorities

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

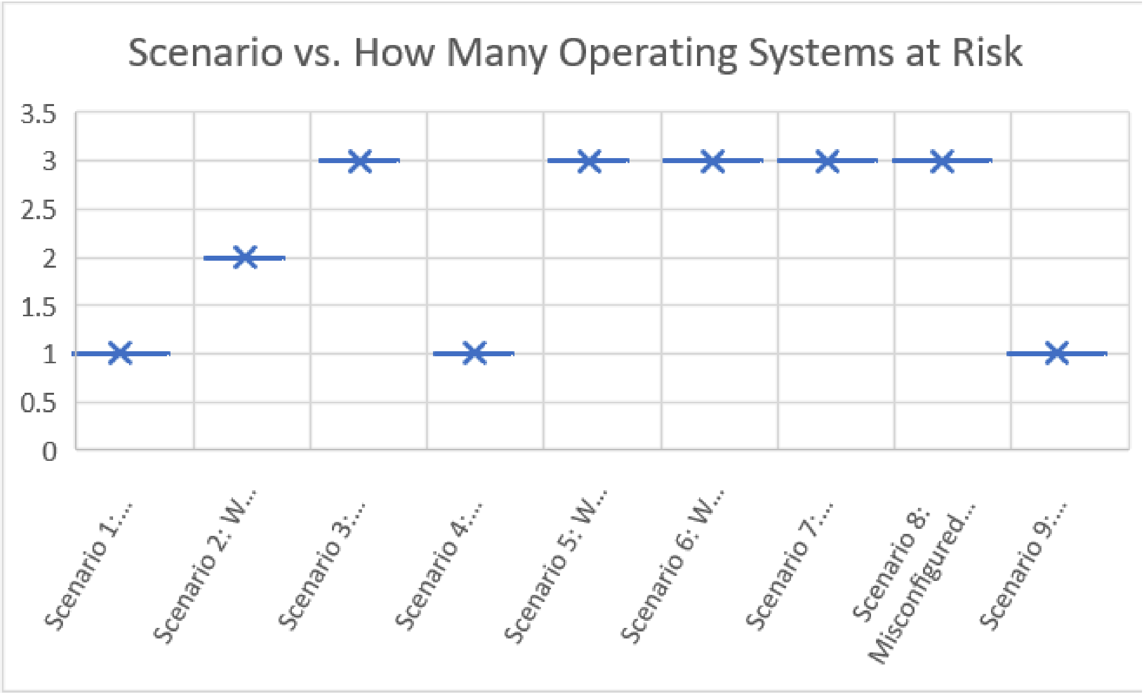
    a. This can be remediated by: Mandating appropriate patches and putting the exchange server within a VPN.

Priority of Solution Implementation

Our office recommends fixing Scenario 2 before any other because of its extremely high CVSS score. This score index is taken from the National Institute of Science and Technology. Because the other scores are also high, but in the same ballpark, we can not recommend prioritization of which of these other vulnerabilities to fix first. They all carry significant risks and our office recommends working on fixing them concurrently.



As a final note, we can see here that different vulnerabilities affect a different number of Operating Systems.


Scenario vs. How Many Operating Systems at Risk
3.5
3
2.5
2
1.5
1
0.5
0
Scenario 1:...
Scenario 2: W...
Scenario 3:...
Scenario 4:...
Scenario 5: W...
Scenario 6: W...
Scenario 7:...
Scenario 8: Misconfigured...
Scenario 9:...