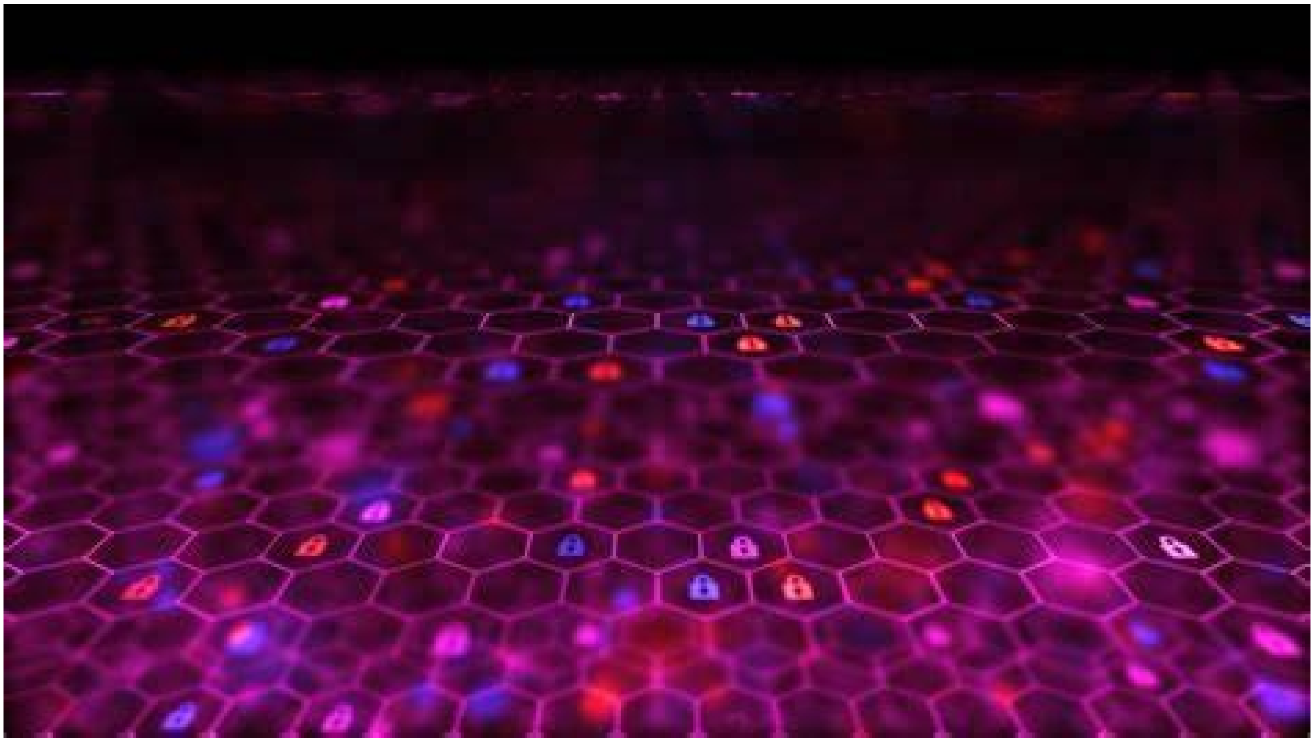


Detailed Technical Report

Rashawn Hill

Table Of Contents

Table Of Contents **2**

Scope Of Work **3**

Project Objectives **3**

Assumptions **4**

Timeline **5**

Summary Of Findings **6**

Recommendations **9**

Scope Of Work

This technical report covers the remote penetration testing of the company Artemis. This test was carried out from a white box perspective, information about device types were given and all other reconnaissance was done using OSINT tools and other resources.

Project Objectives

Build a robust profile on the target during the reconnaissance stage and then create a threat assessment based on vulnerabilities I found after scanning the clients network.Then make an executive summary for the client’s senior management.

Assumptions

We assumed that the following are what we are most likely to encounter when we begin our work.

1. Unpatched RDP is exposed to the internet
2. Web application is vulnerable to SQL Injection
3. Default password on Cisco admin portal
4. Apache web server vulnerable to CVE-2019-0211
5. Web server is exposing sensitive data
6. Web application has broken access control
7. Oracle WebLogic Server vulnerable to CVE-2020-14882
8. Misconfigured cloud storage (AWS security group misconfiguration, lack of access restrictions)
9. Microsoft Exchange Server vulnerable to CVE-2021-26855

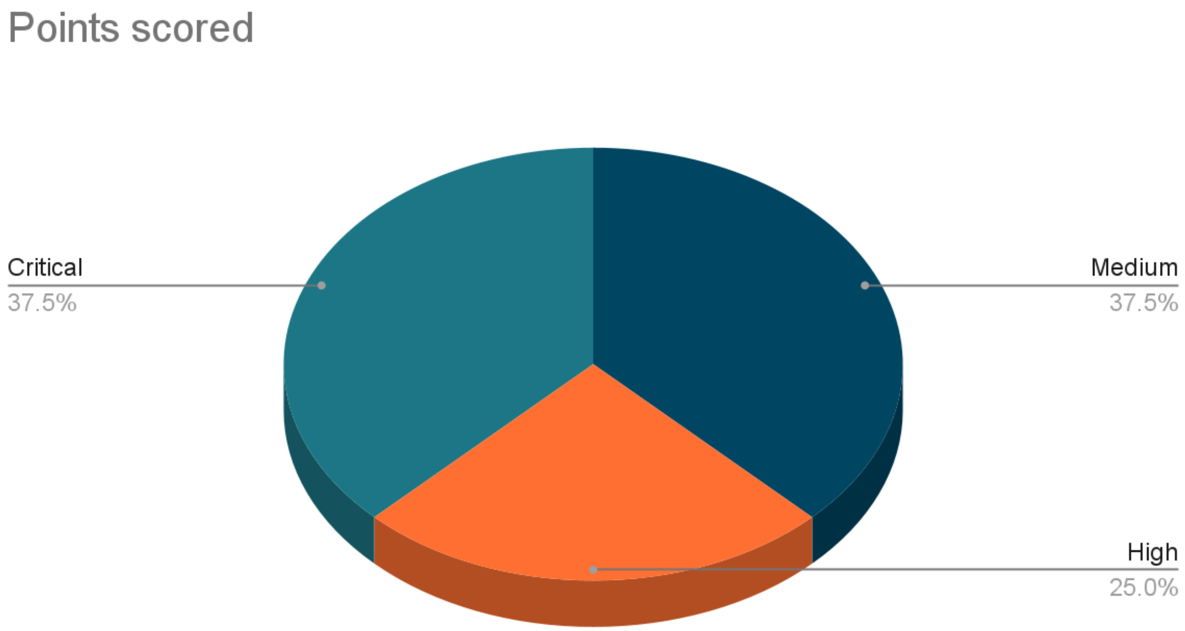
Timeline

Phases	Start date	End date
Reconnaissance	11/12/2021	11/15/2021
Identify targets and run scans	11/16/2021	11/18/2021
Threat assessment	11/19/2021	11/20/2021
Reporting	11/21/2021	11/22/2021

Summary Of Findings

Value	Number of Risks
Low	0

Medium	3
High	2
Critical	3



- I could exploit the flaw to get root privileges using scripts and run commands on vulnerable Apache web servers with limited permissions

- Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server.

- I could exploit this flaw by sending a specially crafted HTTP request to a vulnerable Exchange Server.

- A successful attack could allow any data in the remote MySQL database to be read or modified

- An attacker who successfully exploited this vulnerability could obtain information to further compromise the user’s system.

- A vulnerability in Cisco Ultra Services Framework Element Manager could allow an authenticated, remote attacker with access to the management network to log in to the affected device using default credentials present on the system

  .

- As a result a malicious user can extract sensitive data from the web server and in some cases use this vulnerability in order to get a remote code execution on the remote web server.

Recommendations

- Use regular expressions as whitelists for structured data (such as name, age, income, survey response, zip code) to ensure strong input validation. (secure code)

- If you no longer need these services on your system, consider disabling them as a security best practice. Disabling unused and unneeded services helps reduce your exposure to security vulnerabilities.

- Password management, make sure devices are not using default settings.

- Encrypt data, prevent password attacks, secure authentication gateways

- Install security patches on release.