# *Artemis*

*February 25, 2022*

# Table of Contents

# *Scope of Work*

The scope of work for this project is without boundaries so long as business operations are able to continue without any kind of significant interruption.  Artemis has grown profoundly over the past few years and as such it is of significant importance that the security posture of Artemis is able to keep up with this growth at relatively the same rate.  The operations control group of Artemis monitors over 49,000 data points and the need to make things work has severely outpaced the need to make things work securely.

# *Project Objectives*

The overall objective of this project is to gauge where Artemis stands security-wise and to correct areas that are in need of improvement.  More specifically, this project is a full-blown penetration test consisting of 5 stages, planning and reconnaissance, target identification and scanning, vulnerability scanning, and threat assessment.  After the penetration test is complete Artemis will be armed with the knowledge of what parts of its system is most susceptible, what part is most secure, what part needs just a little more work and what should be kept an eye on. Some of the main concerns going into this penetration test include misconfiguration of older network hardware that is being phased out, misconfiguration of newer network hardware, and overall employee education of security and acceptable use policy.

# *Assumptions*

Due to the need for this to be a very thorough penetration test, not many assumptions were made with the exception of assuming many systems were either misconfigured or in the process of being phased out.

## *Timeline*

**Planning and Reconnaissance:** The planning and reconnaissance phase of the penetration test will take the longest at 2-3 weeks time.  This part will include review of the Rules of Engagement (ROE), as well as the gathering of all information about the target (Artemis).

**Target identification and scanning:** Target identification and scanning to perform host discovery and enumeration will in total take about 1 week.

**Vulnerability assessment:** The identification of all present vulnerabilities in all of Artemis' systems will also take about 1 weeks time.

**Threat assessment:** The threat assessment will take about 1 week to complete.

## *Summary of findings*

In total there were 9 vulnerabilities of note that were found during the penetration test. They are as follows:

**Unpatched RDP is exposed to the internet:** This would give an attacker access to the entire Artemis network.

**Web application is vulnerable to SQL injection:** This is one of the biggest vulnerabilities you will encounter in the wild. If an attacker finds this vulnerability they can gain access to all of your data for all of your customers with only a few SQL commands on a web front end.

**Default password on Cisco admin portal:** It is particularly dangerous to not change your default passwords of your networking hardware as these are well known and can be easily exploited and can be found anywhere from a forum to the dark web. An attacker would be able to manually exfiltrate data from Artemis's systems albeit manually quite easily with this vulnerability.

**Apache web server vulnerable to CVE-2019-0211:** This is a well known vulnerability that primarily affects non Unix systems and causes and if found an attacker can perform arbitrary code execution.

**Web server is exposing sensitive data:** At the end of the day, what a system is doing is protecting data from malicious actors. Broken access control could be a side effect of this vulnerability and clearly sensitive data exfiltration which means you might not be passing your next PCI DSS audit.

**Web application has broken access control:** Depending on the severity a normal user could promote themselves to admin and exfiltrate data. This could also mean some form of an IDOR vulnerability.

**Oracle WebLogic Server vulnerable to CVE-2020-14882:** A very serious vulnerability found in 2020 that affected a large number of Oracle WebLogic Server versions. An unauthenticated user can completely take over the server via HTTP.

**Misconfigured cloud storage (AWS security group misconfiguration, lack of access restrictions):** This can be a variety of things, for example sample applications with known security vulnerabilities were not properly removed. A thorough walkthrough of AWS cloud storage must be performed.

**Microsoft Exchange Server vulnerable to CVE-2021-26855:** This well known vulnerability can allow any attacker to perform SSRF, privilege escalation, and remote code execution.

# *Recommendations*

**Unpatched RDP is exposed to the internet:** With a CVSS score of 6.8, and being a Microsoft protocol the only real fix is to update the system to address this issue.

**Web application is vulnerable to SQL injection:** SQLi protection must be implemented on all front ends this could include character encoding, input validation, secure code review and the use of a fuzzer. This had a CVSS score of 9.3.

**Default password on Cisco admin portal:** This is a very simple but important fix, change all default passwords immediately. This had a CVSS score of 7.3.

**Apache web server vulnerable to CVE-2019-0211:** In order to fix this issue the recommended steps are to update to a more current version of Apache web server. The CVSS score for this is 7.8.

**Web server is exposing sensitive data:** In order to fix this a secure code review must be implemented specifically for an IDOR vulnerability. This has a CVSS score of 5.7.

**Web application has broken access control:** To figure out what is going wrong with access control implement logging, deny by default, and ensure backups and metadata are not present with web roots.

**Oracle WebLogic Server vulnerable to CVE-2020-14882:** In order to fix this well known vulnerability, update to an unaffected version of Oracle WebLogic Server.

**Misconfigured cloud storage (AWS security group misconfiguration, lack of access restrictions):** A number of things need to be done to tie down misconfigured AWS cloud storage. They include changing passwords, implementing least privilege, ACLs, network segmentation, and IaCs.

**Microsoft Exchange Server vulnerable to CVE-2021-26855:** In order to fix this issue Microsoft Exchange Server must be patched and also placed inside a VPN to separate port 443 from external connection requests.