Detailed Technical Report

Artemis Gas, Inc.

Table of Contents

Executive Summary

Scope of Work

This document is a report of the findings of a security assessment performed on ARTEMIS GAS, INC. (“Artemis”). This assessment was performed as an external penetration test.

Project Objectives

The primary objective of this security assessment is to find any potential vulnerabilities or other avenues for exploit in Artemis’ computer systems/networks, and to provide recommendations on how the company can improve its security posture.

Assumptions

The primary assumption made before performing this security assessment was that the networks and web servers were in some way accessible to the testers in order to be able to scan for vulnerabilities and test exploits, whether by already being public networks or by being provided special access for the purposes of completing the test.

Timeline

The penetration test will begin on September 10, 2023, and end on September 24, 2023, lasting 2 weeks in total.

Summary of Findings

Reconnaissance

In the reconnaissance phase of the test, the background information on the company and its computer systems was determined. From a technological standpoint, the organization uses a variety of vendors for hardware and software products. The firewall is constructed of Cisco, Fortinet, and Palo Alto products. The network is composed of Cisco MPLS and Fortigate SD-WAN devices. Load balancing is handled by BIG-IP from F5, and secure remote application access is performed via Zscaler. The company's servers and applications are split evenly between Amazon Web Services (AWS) in the cloud and on-premise, the latter being spread across four major data centers in Houston, Paris, Cairo, and Singapore.

Internal authentication is handled by a Microsoft Active Directory based Single Sign-On (SSO) solution. The company's enterprise resource planning (ERP) system, access to which is authenticated by the SSO solution, runs on Linux and Oracle 12c servers. Internal communications are done via Microsoft Exchange, through a blend of Exchange Online via Office 365 cloud tenant and on-premise Microsoft Exchange servers. The SSO solution also grants access to PARS, a system for engineers to submit technical information regarding potential patents, and APOLLO, a repository for sensitive trade secrets.

Vulnerability Assessment

CVSS Label	CVSS Score
none	0.0
low	0.1-3.9
medium	4.0-6.9
high	7.0-8.9
critical	9.0-10.0

The chart to the left shows the Common Vulnerability Scoring System (CVSS) labels assigned to each range of severity scores. There were nine main vulnerabilities uncovered over the course of this assessment, of varying degrees of severity. The chart below shows the breakdown of the severity classes of the vulnerabilities that were discovered. Some of the vulnerabilities may vary in severity depending on context, so the “Low Estimate” column corresponds to the best-case scenario and the “High Estimate” column corresponds to the worst-case scenario.

Severity	Risks (Low Estimate)	Risks (High Estimate)
none	0	0
low	0	0
medium	1	0
high	4	2
critical	4	7

Unpatched RDP is exposed to the Internet. At least one known and documented vulnerability exists in the code of the version of RDP being used, and it is accessible from the Internet to a remote attacker. This issue can affect multiple versions depending on what specific vulnerability is causing it; any unpatched version is at risk. If successful, an attacker can access and control accounts on the system, including potentially root or other admin-privileged account. In attempting to exploit the vulnerability, an attacker could cause

degradation of performance and unintentional denial of service or account lockout due to limited licenses. Depending on the specifics, the CVSS score for this is 8-9 (high).

Web application is vulnerable to SQL injection. The product constructs all or part of a SQL command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended SQL command when it is sent to a downstream component. This is a programming implementation error, so it can affect any version. An attacker can bypass security checks, insert additional statements that modify the back-end database, possibly including execution of system commands, view data stored in the SQL database, modify or delete information, or inject and run malicious code on the server. Sending a malformed request can also cause the system to crash or hang, leading out outages. This has a CVSS score of 8-9 (high).

Cisco administration portal is using the default password. Many devices are shipped with default credentials -- such as username and password both being “admin” -- and users frequently do not know or do not bother to change it. These credentials are easy to find online. This is a configuration mistake, so it can affect any version. If successful, an attacker could take down the system completely, change the password and turn it off, requiring a physical reboot. They could also change credentials or network pathways, such as by setting up a redirect to a malicious website. In attempting to exploit this the attacker could boot or prevent real admins from logging in; if there are multiple possible default passwords, or they are scanning for the vulnerable routers, there could be an unintentional denial or degradation of service as they brute force their way through. This has a CVSS score of 9-10 (critical).

Apache web server is vulnerable to CVE-2019-0211. Code executing in less-privileged child processes or threads, including scripts executed by an in-process scripting interpreter, could execute arbitrary code with the privileges of

the parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected. This vulnerability specifically affects Unix-based Apache HTTP Server 2.4, releases 2.4.17-2.4.38. A successful attacker can run malicious code, potentially with root privileges, and a malformed request can cause the system to crash or hang. This has a CVSS score of 7.8 (high).

Web server is exposing sensitive data. The product exposes sensitive information to an actor that is not explicitly authorized to have access to that information. This could affect any number of versions, as it depends on which specific vulnerability is causing this problem. An attacker could scrape credentials, data, and personally identified information (PII), and could potentially introduce ransomware if they are able to acquire write privileges. If an attacker is scraping lots of data, there would be denial or degradation of service; scraping tons of basic information will involve going through many pages, whereas scraping bigger files, even if in a smaller quantity, will use up the bandwidth. This has a CVSS score of 9 (critical).

Web application has broken access control. Attackers can access, modify, delete or perform actions outside an application or systems' intended permissions. This vulnerability could have different causes, but it is usually a configuration error, so it can affect any version. A successful attacker will gain unauthorized access; degree can vary. For example, an employee who is able to open a folder they shouldn't have access to is likely not that serious and would have a CVSS score of 4-5 (medium), but an external attacker able to gain control of an admin account with root privileges would get a CVSS score of 10 (critical). A malicious attacker constantly trying to access sensitive locations, shared drives, etc. may cause lowered performance due to their activities.

Oracle WebLogic Server is vulnerable to CVE-2020-14882. This easily exploitable vulnerability allows an unauthenticated attacker with network access via HTTP to compromise the server. This specific vulnerability affects Oracle

WebLogic Server versions 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. Successful attacks of this vulnerability can result in takeover of the Oracle WebLogic Server, and malformed requests can cause the system to crash or hang. This has a CVSS score of 9.8 (critical).

Cloud storage is misconfigured. Some part of the cloud storage solution was misconfigured in a way that introduces security vulnerabilities (this could have any number of causes, such as AWS security group misconfiguration or lack of access restrictions). Because this is a configuration error, it may affect any version. An attacker could gain access to the OS, virtual resources, firewalls, etc. Depending on the attack, there are also other risks, such as global write allowing the storage to be used up. An attacker could also be storing illegal content or malware that would then be traced back to the legitimate server owner. Global read can cause denial or degradation of service from someone connecting and scraping tons of data. Basic information will involve going through many pages whereas bigger files will use up bandwidth. This has a CVSS score of 7-8 (high).

Microsoft Exchange Server is vulnerable to CVE-2021-26855. This is a remote code execution vulnerability. It affects unpatched Microsoft Exchange Server 2013, 2016, and 2019. This includes a type of server-side request forgery (SSRF), so an attacker could run malicious scripts on the server, potentially using it as a point of attack or pivot. They could also download emails or write to files, and a malformed request could cause the system to crash or hang. This has a CVSS score of 9.8 (critical).

Recommendations

Overall, keep things patched and up-to-date. Several of the vulnerabilities discovered are already well documented and patches exist that solve the issue, so these should be installed as soon as possible. More generally, implement a policy of regularly checking for security updates and patches for the software (and hardware/firmware) being used and installing them in a timely manner.

Unpatched RDP is exposed to the Internet. Use single sign-on (SSO), multi-factor authentication/2-factor authentication (MFA/2FA), and/or password management systems. In the short term, patch RDP immediately.

Web application is vulnerable to SQL injection. Write more secure code that sanitizes user input by properly neutralizing special elements before sending the query to the server. Consider using an external library for this. In general, train staff -- especially developers -- in secure coding best practices so they are aware of these types of problems and how to avoid them.

Cisco administration portal is using the default password. Very simply, change the password immediately. Changing default passwords upon setup should be part of the organization-wide password management policy.

Apache web server is vulnerable to CVE-2019-0211. Update the web server and install any available patches.

Web server is exposing sensitive data. Remediation depends on what precisely is causing the data leak, but in general, focus on data protection and data loss prevention, encrypt sensitive data at rest (on hard drives) and in transit, use secure, strong credentials, and fix any potential issues with permissions and access control.

Web application has broken access control. If the issue is on a service provider’s side (such as Okta or something similar), upgrade to the newest version and/or install any available patches. If the error is on the internal side, make sure

clear policies and best practices are being followed and make sure the product is being tested before being deployed. Always apply the principle of least privilege: only grant access to those who truly need it to be able to perform their duties. That way, an attacker will be denied by default.

Oracle WebLogic Server is vulnerable to CVE-2020-14882. Update the server and install any available patches.

Cloud storage is misconfigured. Ensure secure builds and documentation exist and are being followed. Have the solution audited, run vulnerability scans regularly, and compare to security standards to ensure they match.

Microsoft Exchange Server is vulnerable to CVE-2021-26855. Update the server and install any available patches.