

Well Architected Framework Assessment

November 12, 2024

Christopher Shrout

Principal Analyst, Sequoia Inc.

Contents

[Overview 3](#_Toc184886377)

[Assessment Scope 4](#_Toc184886378)

[Reconnaissance 5](#_Toc184886379)

[Server/Infrastructure Findings 6](#_Toc184886380)

[Primary Server/Infrastructure Findings 6](#_Toc184886381)

[Application Findings 8](#_Toc184886382)

[Primary Application Findings 8](#_Toc184886383)

[AWS Findings 10](#_Toc184886384)

[Primary AWS Findings 10](#_Toc184886385)

[Conclusion and Recommendations 14](#_Toc184886386)

[Recommendations 14](#_Toc184886387)

[Appendix A: Server / Infrastructure Findings 15](#_Toc184886388)

[Appendix B: Application Findings 19](#_Toc184886389)

[Appendix C: AWS Findings 22](#_Toc184886390)

# Overview

This penetration test was conducted against the Combine development environment and Combine Dashboard between October 21st, 2024 and November 12th, 2024. Three primary categories were assessed: AWS, infrastructure, and application. This assessment was conducted at various layers using industry standard tools. Both automated and manual checks were conducted; tests for inappropriate permissions, injection vulnerabilities and public internet access were run.

The primary findings are as follows:

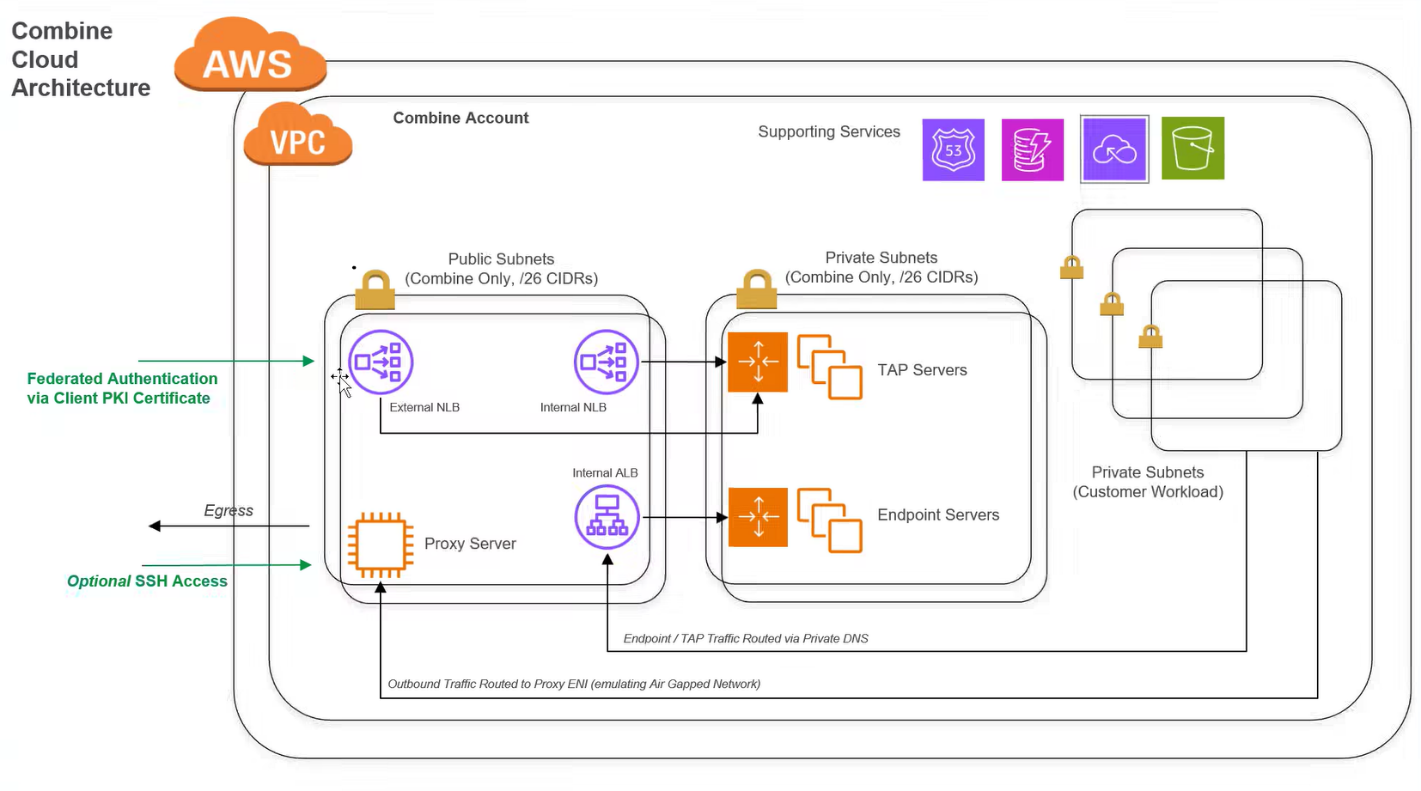
* AWS:
  + 65 high criticality findings
  + 39 medium criticality findings
  + 87 low criticality findings
* Server/Infrastructure
  + Root privileges assigned to the default ec2-user account
  + Inbound & outbound public internet access on dashboard
  + SSH redirection allowed on bastion host
  + Lack of application whitelisting
  + Presence of outdated software within the environment.
* Application
  + High-privileged ‘ec2-user’ account is used to host a publicly available website.
  + Content from the Combine dashboard is served to unauthenticated users
  + Slightly out of date software is being used to host the Combine dashboard
  + The server software version is present in error messages

The Combine application proves to be difficult to access from the outside. Client certificate authentication is required to view the full Combine dashboard. Console connections to the server environment require SSH certificates. Lateral movement to the Combine dashboard server over SSH requires an additional SSH certificate. The dashboard web application has very few input fields, all of which proved resistant to injection attack. Reconnaissance on Combine does not reveal the URL or public IP of any existing Combine installation.

The primary weaknesses for Combine involve its broad public access to the site, lack of rules and reporting for inbound and outbound traffic and inappropriate use of privileged users to run hosted services. See the report body for more information; appendices also exist for each section of the report. The appendices outline exact details of each finding and potential mitigations where available.

All findings have been addressed; mitigations have been implemented where necessary and plans for future mitigations are in place. Certain findings remain open, pending the customer’s decision to close them.

# Assessment Scope



The scope of this assessment included the following IP address ranges and systems:

* Publicly accessible demonstration Combine dashboard URL (TAP Servers):
  + <https://combine-1-elb-tap-e-ed11d741df7f5cd4.elb.us-east-1.amazonaws.com>
* Internal network targets:
  + Bastion host (AKA Proxy Server) accessed via SSH: 10.0.0.20
  + Test system: 10.0.241.211
  + Combine dashboard systems (TAP Servers): 10.0.0.0/24
    - AWS load balancers dynamically create dashboard instances each day, assigning a new IP address within the 10.0.0.0/24 subnet each time.

# Reconnaissance

Basic reconnaissance was performed on Sequoia’s Combine software yielding very little information.

A whiteboard with writing on it

Description automatically generated with medium confidence

The basic network architecture is outlined in a promotional YouTube video, along with the names of various C suite personnel from Sequoia.

The following Combine related URLs were found:

* <https://aws.amazon.com/marketplace/pp/prodview-hfz6xwelgmzpu>
* <https://www.sequoiainc.com/combine>
* <https://youtu.be/ZJ23A8zzW3A>

The Combine demo URL could not be identified using Google and matching keywords.

# Server/Infrastructure Findings

Server and infrastructure findings were identified using SSH, NMAP and built in CLI utilities. All analysis was conducted manually using remote access to the Combine systems.

Access to the internal network was provided via a generated private key and a publicly available domain name. The Combine bastion host serves an SSH connection at the specified URL. Connecting to the bastion host over SSH requires use of the privately generated key. Once connected to the bastion host, it is possible to use SCP to transfer files back and forth from the system. A statically compiled copy of NMAP was uploaded on to the bastion host for use enumerating the internal network structure. Once neighboring systems were discovered, it was possible to use SSH redirection to expose internal network ports through to the attacking system. Additional ssh ports were discovered within the 10.0.0.0/24 subnet and the 10.0.241.211 systems. Attempts were made to connect to the other internal systems using the provided private key. A successful SSH connection was also made to 10.0.241.211.

Primary Server/Infrastructure Findings:

1. **Public application with root privilege:** Within the Combine dashboard server, the default ‘ec2-user’ is utilized on the Apache Tomcat service. Tomcat runs the publicly accessible Combine Dashboard. With the current configuration, the ‘ec2-user’ account has sudoer privileges on all accessible systems and can escalate privilege with no password. To resolve this issue a dedicated, lower-privileged service account should be used to host the dashboard application.
   * **Mitigation:** A lower privilege account will be used in the 3.14 release.
2. **Server content is publicly available:** The Apache Tomcat server publicly displays an error page to users connecting without a client certificate. This makes it possible for an attacker to compromise the underlying ec2-user account from the broader internet. A compromise of this type would require a vulnerability within the web application itself. Should this account be compromised, it would have immediate privileged access to the hosting server.
   * **Mitigation:** This error page is necessary for user troubleshooting and will not be removed.
3. **Outbound HTTP connections allowed:** The Combine dashboard server allows outbound HTTP requests to the broader internet using curl. These connections are not reported in the migration violations dashboard within Combine. Malware downloads and command & control channels most commonly utilize HTTP connections.
   * **Mitigation:** Changes in outbound connectivity are being evaluated for the 3.14 release.
4. **No application whitelisting:** No application whitelisting is present on the bastion host to prevent the execution of unapproved binary files. This was demonstrated through the statically compiled NMAP binary placed on the system and used. Only the bastion host was tested for the use of outside binaries.
   * **Mitigation:** Application whitelisting cannot be implemented as Combine is intended for use as a development environment.
5. **SSH redirection:** A second private key is necessary to connect to the SSH console on the Combine dashboard server. After being provided with this key it was then possible to redirect the SSH connection to the dashboard server through the bastion host.
   * **Mitigation:** This is considered necessary functionality for accessing the environment and will not be changed.
6. **Outdated Operating System software:** The bastion host, internal SSH server and Combine dashboard server all display the following message when accessed via the console:

|  |
| --- |
| A newer release of "Amazon Linux" is available.  Version 2023.6.20241028:  Version 2023.6.20241031:  Run "/usr/bin/dnf check-release-update" for full release and version update info |

* + **Mitigation:** OS updates are applied during installation and can be performed as needed. Post-deployment, it is considered a best practice for customers to schedule and carry out regular OS updates. The current demo environment will be patched to the latest OS version.

See [Appendix A: Infrastructure Findings](#_Appendix_B:_Server) for additional information and findings regarding the environment hosting the Combine web application.

# Application Findings

Primary findings regarding the Combine dashboard application relate to the ability for unauthenticated users to access content hosted by the server and information available within the application for authenticated users. The application itself was tested using OWASP’s Zed Attack Proxy (ZAP) and various curl commands.

ZAP was configured for mutual authentication to the Combine dashboard page using a pre-generated client certificate. ZAP was then set up as a local proxy through which system applications and utilities could access the site without supporting client authentication. ZAP’s active scan, spider and forced browse functionality were all used to explore the site and find potential vulnerabilities.

The Combine dashboard application is running on an Apache Tomcat 10.1.24 server within an Amazon Linux 2023.6.20241010 instance. The Tomcat software is executed from the ‘/opt/tomcat/tomcat.jar’ file with its backend data being stored in AWS hosted DynamoDB tables. The Tomcat server is being run by the privileged ‘ec2-user’ on the underlying system.

Primary Application Findings:

1. **Unauthenticated access to content served with root privilege:** An unauthenticated user is presented with an “error.html” page hosted by the Apache Tomcat 10.1.24 server. Should a vulnerability exist allowing remote code execution via limited access to the server, an attacker would have immediate privileged access to the server via the ‘ec2-user’ identity. It may not be necessary to host an error page when user authentication fails, rather the server can simply stop serving content.
   * **Mitigation:** A low privileged user will run the Apache Tomcat server in the 3.14 release. “error.html” must remain for end user troubleshooting.
2. **Content exposed to authenticated users:** An authenticated user can enumerate several subdirectories or URI’s (Uniform Resource Indicators) beneath the main Combine dashboard. Of minor concern is the presence of the “metadata” URI wherein the user can see settings for a variety of AWS services within their environment. Unless necessary for Combine’s purpose, this URI should be restricted to only services or accounts that require it.
   * **Mitigation:** This will be addressed in the 3.14 release.
3. **Out of date software:** The installed Apache Tomcat 10.1.24 server is slightly out of date. CVE 2023-34750 relates to an embedded core version of Tomcat 10.1.24 that is vulnerable to resource exhaustion due to unclosed HTTP/2 streams. The server should be updated to the latest version.
   * **Mitigation:** This will be addressed in the 3.14 release.
4. **Server version in error messages:** The server version is present in error messages. Hiding this information makes it slightly more difficult for an attacker to determine the exact version of the underlying server.
   * **Mitigation:** This issue will be evaluated prior to the 3.14 release.

See [Appendix B: Application Findings](#_Appendix_C:_Application) for additional information and findings regarding the Combine web application.

# AWS Findings

The Prowler security tool was used to conduct an audit of the Combine AWS (Amazon Web Services) Environment. All findings relate to AWS’ “Well Architected Framework” compliance requirements. These requirements are all in relation to the security of the configurations present within the assessed AWS environment. The findings follow below:

|  |  |  |
| --- | --- | --- |
| **Criticality** | **Number of Categories** | **Total Findings** |
| **High** | 8 | 65 |
| **Medium** | 5 | 39 |
| **Low** | 7 | 87 |

High criticality categories are covered in this section of the report. Note that the same finding may be present on multiple resources, increasing the overall finding count. Findings deemed to be “not applicable” have not been included in the count. See Appendix C: AWS Findings for full detail on all findings. Pertinent findings are below:

Primary AWS Findings:

1. **SEC01-BP02:** Multi-factor authentication (MFA) is not enabled for the root account.

**Mitigation:** This is not controlled via the Combine application and therefore does not apply.

1. **SEC02-BP01:** Password complexity, length and reuse need to be reviewed. The following resources do not use multi-factor authentication:
   1. combine\_provisioning

**Mitigation:** This is not controlled via the Combine application nor is it a part of the Combine baseline, therefore it does not apply. This user is created by the customer and is managed by the customer.

1. **SEC02-BP02:** User ‘combine\_provisioning’ has not rotated access key 1 in 682 days (at the time of testing)

**Mitigation:** This is not controlled via the Combine application and therefore does not apply. This user is created by the customer and is managed by the customer.

1. **SEC02-BP04:** The following resources could be affected by a cross-service confused deputy attack.
   1. Combine-I-Bastion
   2. Combine-I-CFN-CR-ConfigurationValue
   3. Combine-I-CFN-CR-ConfigureCombineFirewall
   4. Combine-I-Debug-Server
   5. Combine-I-Endpoints
   6. Combine-I-LogIngest
   7. Combine-I-LogListener
   8. Combine-I-Proxy
   9. Combine-I-Tap
   10. Combine-S-WLDEVELOPER-EC2
   11. Combine-TS-WLDEVELOPER-EC2

**Mitigation:** Changes to these resources will be evaluated prior to the 3.14 release.

1. **SEC03-BP01:** Instance i-00b4c9718c3da677f has IMDSv2 (Instance Metadata Service Version 2) disabled or not required. This protocol helps protect against Server-Side Request Forgery.

**Mitigation:** These changes will be evaluated prior to the 3.14 release. These changes will only be made if required in a customer environment.

1. **SEC04-BP01:** Service and application logging needs to be configured & retained.
   1. Account 776492542696: No CloudTrail trails have a data event to record all S3 object-level API operations.

**Mitigation:** This is not applicable as it is not controlled by the Combine application. The customer shares responsibility for configuration.

* 1. The following lambda functions are not recorded by CloudTrail.
     1. Combine\_CFN\_CF\_Configuration\_Value
     2. Combine\_CFN\_CF\_Configure\_Combine\_Firewall
     3. Combine\_Log\_Ingest
     4. Combine\_Log\_Listener\_Firewall

**Mitigation:** These changes will be evaluated prior to the 3.14 release.

* 1. The following resources do not have access logs configured:
     1. Combine-1-ELB-Endpoints
     2. Combine-1-ELB-Tap-E
     3. Combine-1-ELB-Tap-I

**Mitigation:** These changes will be evaluated prior to the 3.14 release.

* 1. The following resources have server access logging disabled
     1. cf-templates-1ueme6jh7wt3e-us-east-1
     2. combine-app-storage-776492542696
     3. combine-app-storage-776492542696-public
     4. combine-connection-logging-us-east-1-776492542696
     5. combine-devops-776492542696
     6. combine-devops-776492542696-us-east-1

**Mitigation:** Combine supports this functionality as an optional feature that can be enabled by customers if desired.

* 1. vpc-042445bc36ec4511b: VPC Combine Flow logs are disabled.

**Mitigation:** These changes will be evaluated prior to the 3.14 release.

1. **SEC04-BP02:** Account 776492542696 has AWS Config recorder disabled and “CloudTrail trails enabled with logging” is not found for this account. The endpoint vpc-042445bc36ec4511b has VPC Combine Flow logs disabled.

**Mitigation:** This is not applicable as it is not controlled by the Combine application. The customer shares responsibility for configuration.

1. **SEC05-BP01:** The following VPC endpoints can be accessed from non-trusted accounts:
   1. vpce-03492d36b0d2941aa
   2. vpce-0388bcb8177ab50bc
   3. vpce-07ffb13b2ec06bb9e
   4. vpce-0f2c7418733cb3d50

**Mitigation:** These endpoints were manually created and are not a part of the Combine baseline.

1. **SEC05-BP02:** Configure network segments appropriately; all access between the internet and various internal subnets requires proper configuration.
   1. acl-0e3497a8b874acd2c: Port 22 is open to the internet
   2. The following resources have bucket ACLs and ‘MFA Delete’ disabled:
      1. cf-templates-1ueme6jh7wt3e-us-east-1
      2. combine-app-storage-776492542696
      3. combine-app-storage-776492542696-public
      4. combine-devops-776492542696
   3. The following resources have ‘MFA delete’ disabled:
      1. combine-connection-logging-us-east-1-776492542696
      2. combine-devops-776492542696-us-east-1

**Mitigation:** These are necessary settings for the environment; these settings will not be changed.

1. **SEC06-BP01:** Frequent scanning and patching for vulnerabilities needs to occur.
   1. i-00b4c9718c3da677f: IMDSv2 is disabled or not required.
   2. i-03b14bacecc04b262c
      1. internet facing IP of 52.70.28.12
      2. Internet facing Instance Profile arn:aws:iam::776492542696:instance-profile/Combine-I-Bastion

**Mitigation:** Software will be deployed at the latest version; however, it is recommended as a best practice for the customer to conduct scans within their environment post-deployment.

1. **SEC08-BP02:** Enforce encryption at rest.
   1. The following resources do not have AWS KMS (key management system) keys associated
      1. /aws/eks/combine-test/cluster
      2. /aws/lambda/Combine\_CFN\_CF\_Configuration\_Value
      3. /aws/lambda/Combine\_CFN\_CF\_Configure\_Combine\_Firewall
      4. /aws/lambda/Combine\_Log\_Ingest
      5. /aws/lambda/Combine\_Log\_Listener\_Firewall
      6. /aws/lambda/Combine\_Log\_Listener\_Proxy
      7. /aws/lambda/Combine\_Log\_Listener\_Proxy\_FlowLogs
      8. Combine\_Log\_Group\_Endpoint
      9. Combine\_Log\_Group\_Firewall
      10. Combine\_Log\_Group\_Proxy\_Flow\_Logs
      11. Combine\_Log\_Group\_TAP
      12. Test

**Mitigation:** Changes to these resources will be evaluated prior to the 3.14 release.

* 1. Account 776492542696: Elastic Block Store (EBS) Default Encryption is not activated.

**Mitigation:** Combine supports this functionality as an optional feature that can be enabled by customers if desired.

* 1. EBS vol-0b089897f788c5663: EBS Snapshot vol-0b089897f788c5663 is unencrypted.

**Mitigation:** Combine supports this functionality as an optional feature that can be enabled by customers if desired.

1. **SEC09-BP02:** Enforce encryption in transit.
   1. The following resources do not have a bucket policy, allowing HTTP requests:
      1. cf-templates-1ueme6jh7wt3e-us-east-1
      2. combine-app-storage-776492542696
      3. combine-app-storage-776492542696-public
      4. combine-devops-776492542696
      5. combine-devops-776492542696-us-east-1
   2. Combine-1-ELB-Endpoints
      1. ELBv2 ALB Combine-1-ELB-Endpoints has non-encrypted listeners.
      2. ELBv2 Combine-1-ELB-Endpoints has listeners with insecure SSL protocols or ciphers (ELBSecurityPolicy-2016-08).
   3. combine-connection-logging-us-east-1-776492542696: allows requests over insecure transport in the bucket policy.

**Mitigation:** Changes to these resources will be evaluated prior to the 3.14 release.

1. **SEC10-BP01:** Account 776492542696: AWS Support Access policy is not attached to any role.

**Mitigation:** This resource is not within the scope of control of the Combine application.

See [Appendix C: AWS Findings](#_Appendix_C:_AWS) for additional information and findings regarding the Combine web application.

# Conclusion and Recommendations

Mutual authentication implemented by Combine makes it exceedingly difficult to enumerate vulnerabilities without authorized access. The requirement for private certificates to authenticate to Combine’s SSH interfaces makes unauthorized access extremely unlikely. Use of additional certificates to access Combine’s dashboard server within the internal AWS infrastructure makes lateral movement to the dashboard extremely challenging. The DynamoDB back end of the application makes traditional SQL injection attacks irrelevant. Any successful injection attacks would require the use of NOSQL techniques, likely specific to DynamoDB.

Primary weaknesses in Combine’s current configuration include the ability to access hosted content anonymously on the dashboard server from the public internet and elevated privileges assigned to the default ec2-user. Should the Tomcat server become compromised, an attacker would instantly gain privileged access to the underlying server. Additionally, one other system inside of the demonstration environment (10.0.241.211) allows for SSH access using the same private key.

Many recommendations have been made by Prowler cloud security software. This specific instance of Combine is used as a demonstrator for sales purposes only. It is possible for any customer to modify their cloud configuration to increase compliance with AWS’ “Well Architected Framework” guidance.

## Recommendations

The following recommendations will improve the security posture of the Combine server installation:

1. Create a dedicated, minimal privilege account to host the Combine web application.
2. Do not serve web content to any user that fails client certificate authentication.
3. Require a password in addition to a user certificate when connecting to the bastion host and internal Combine systems over SSH.
4. Require a password for privilege escalation on the console of all Combine systems.
5. Restrict SSH redirection on the bastion host as required
6. Only use the bastion host SSH certificate for authentication to the bastion host.
7. Application whitelisting should be implemented, at least on the bastion host
8. Regularly patch and update all Combine software.

# Appendix A: Server / Infrastructure Findings

Server infrastructure was assessed using SSH, NMAP and built in CLI utilities. Access was granted to a demonstration version of Combine’s bastion host and tap server. Infrastructure findings were generated manually via enumeration of settings within Combine’s systems. Service discovery on adjacent hosts was conducted with a statically compiled copy of NMAP moved on to the bastion host via SCP.

Combine’s internal network architecture changes daily, being auto generated by AWS at the start of each day. Most systems under configuration control reside within the 10.0.0.0/24 subnet. Two hosts are statically configured including the AMI server at the IP Address 10.0.211.241 and the bastion host (ssh connection from outside of the network) at 10.0.0.20. All systems outside of these IP addresses and ranges are under the configuration control of AWS.

The following concerns were identified within the Combine demo infrastructure:

1. Privilege Escalation is automatic for the ec2-user on all accessible systems.
   1. ‘etc/sudoers’ references the ‘/etc/sudoers.d’ directory:

|  |
| --- |
| ## Read drop-in files from /etc/sudoers.d (the # here does not mean a comment)  #includedir /etc/sudoers.d |

* 1. Within ‘/etc/sudoers.d’ is a file titled ’90-cloud-init-user’

|  |
| --- |
| # Created by cloud-init v. 19.3-46.amzn2 on Fri, 09 Dec 2022 16:57:41 +0000  # User rules for ec2-user  ec2-user ALL=(ALL) NOPASSWD:ALL |

* 1. This configuration causes the ec2-user to not require a password
     1. This is true for the bastion host (10.0.0.20), the tap server and the AMI server (10.0.211.241)

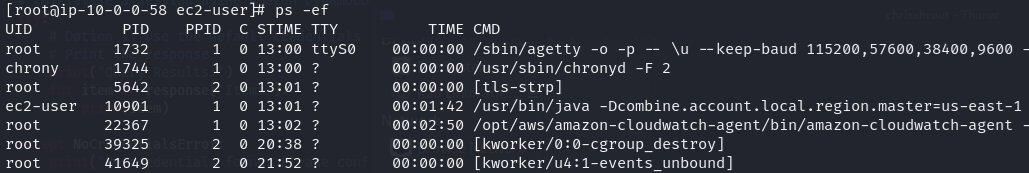
**Mitigation:** A fix for this is being evaluated prior to the release of version 3.14.

1. Combine software on the tap server is running as the ec2-user with sudoer permissions
   1. netstat -pantu indicates the same process ID hosting services on port 8080 and 8443 as the java process on the system being executed by the ec2-user

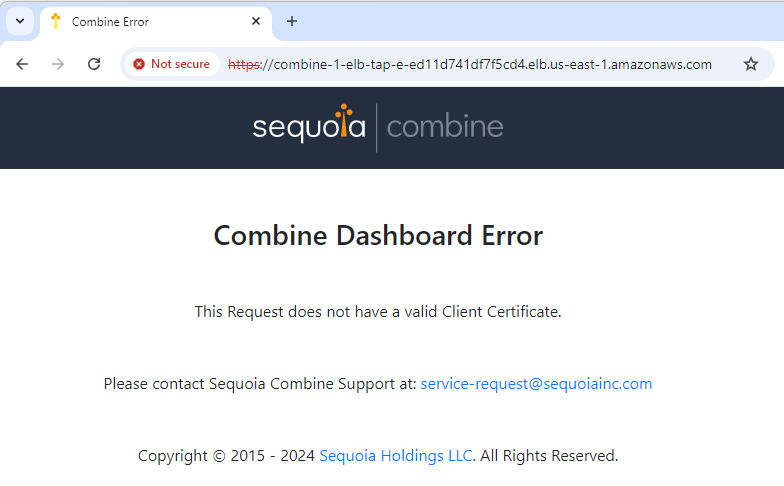
A black screen with white text

Description automatically generated with low confidence

ps -ef output shows that a java application with ‘Combine’ arguments is running on the indicated PID



* 1. Even without an appropriate client certificate for authentication to the web server an anonymous user can load the Combine error dashboard page



**Mitigation:** This error page is necessary for end-user troubleshooting and cannot be removed.

* 1. Should an attacker gain access to the user hosting the Apache Tomcat server they will have full sudoer access to the underlying system immediately.

**Mitigation:** ec2-user will no longer be used to run the Tomcat server in Combine version 3.14.

1. Outbound HTTP connections are allowed from the Combine Dashboard server:

Text

Description automatically generated

* 1. After establishing a redirected SSH connection in to the Combine dashboard server it was possible to download the google.com webpage using the curl command.
  2. This action did not appear in the migration violations dashboard:

Graphical user interface, text, application

Description automatically generated

**Mitigation:** Modifications to policy regarding internally generated outbound connections will be evaluated prior to the 3.14 release.

1. SSH redirection from the bastion host to 10.0.211.241 using the same certificate for the bastion ec2-user allows for SSH access on to the remote system:
   1. Due to the lack of authentication for privilege escalation anyone with the “ec2-user’ identity will have immediate root access on both systems

**Mitigation:** This is by design and will not be changed.

1. Non-approved binary execution
   1. A statically compiled copy of NMAP was moved on to the bastion host and placed inside the home directory of the “ec2-user” account.
   2. No systems are in place to prevent the execution of binary files that have not been approved.

**Mitigation:** This is by design and will not be changed; Combine is a development platform and must allow for the execution of customer created binaries without whitelisting.

1. Out of date operating systems
   1. Upon connecting to the bastion host the following message is displayed:

A newer release of "Amazon Linux" is available.

Version 2023.6.20241028:

Version 2023.6.20241031:

Run "/usr/bin/dnf check-release-update" for full release and version update info

* 1. Publicly facing operating systems and all associated packages should be updated as soon as possible upon the release of newer versions.

**Mitigation:** Updates are performed on a quarterly basis and operating systems can be updated at any time. The current demo environment will be patched to the latest OS.

# Appendix B: Application Findings

OWASP ZAP, sqlmap, curl and FireFox were all used in the assessment of the Combine Dashboard web application. The findings are as follows:

1. Failed client certificate authentication still yields a page publicly hosted by the underlying server.
   1. The ‘ec2-user’ hosting the Combine server has privileged access to the operating system by default.
   2. It is not necessary to serve content after client authentication fails.

**Mitigation:** This page is necessary to facilitate end user troubleshooting. This functionality will not be changed.

1. Out of date Apache Tomcat 10.1.24 server.
   1. CVE-2024-34750 allows for unchecked resource consumption when HTTP2 connections are made to unpatched versions of Apache Tomcat servers.
   2. Apache Tomcat should be upgraded to the latest version, 10.1.25 to resolve this vulnerability.

**Mitigation:** This will be addressed in the version 3.14 release.

1. Forced Browsing
   1. Utilizing “directory\_list\_lowercase\_2.3-big.txt” in a forced browsing attack on the “/tap/api/v1” URI yielded the following “hidden” URI’s:
      1. “/tap/api/v1/metadata
         1. This appears to be a list of server configurations for rewriter request/response and filters.
         2. These appear to be related to the state of various AWS services.

Graphical user interface, text, application, email

Description automatically generated

* + - 1. If this information is not necessary for the functioning of the web application it should be hidden from regular users.

**Mitigation:** This will be addressed in the version 3.14 release.

* 1. It should be noted that some error messages reveal the server software and version number:

Graphical user interface, text, application, email

Description automatically generated

* + 1. Typically, modification of the server.xml file located in the <tomcat directory>/conf can hide the version number from error messages.
       1. Look for the “host” tag and enter the following information:
       2. <Valve className="org.apache.catalina.valves.ErrorReportValve" showReport="false" showServerInfo="false"/>
    2. There is no ‘server.xml’ file present within Combine’s ‘/opt/tomcat/conf’ directory nor the ‘/opt/tomcat/tomcat.jar’ file.
       1. Root cause analysis needs to be conducted to determine exactly where this error message is being generated.
    3. If the version of Tomcat is up to date, then this is not a major concern.

**Mitigation:** This will be evaluated prior to the version 3.14 release.

The following findings proved to be false positives; however, they are recorded in this appendix as OWASP ZAP alerted on them. The finding and its resolution are listed here.

1. SQL Injection attacks
   1. As Combine utilizes DynamoDB most traditional RDBMS SQL injections attacks will not work.
   2. OWASP ZAP returned alerts for several blind timing-based attacks. Listed below are the URIs:
      1. /tap/api/v1/config/application
      2. /tap/api/v1/servers
      3. /tap/api/v1/users
      4. /tap/api/v1/users/407###
         1. This was the user ID of the tester
      5. /tap/api/v1/users/current
      6. /tap/api/v1/violations
   3. CURL requests were made directly to these URIs using timing-based injection attack techniques.
      1. These attacks had no effect.
   4. The “config/application” URI returns an error 405, denying the user access to the resource.
   5. Server data returns empty; an additional URI may be required to invoke a response.
   6. User information returned for the current user is necessary for login purposes
      1. Modifying the requested ID in the “/tap/api/v1/users/407###” URI yields a 401 error message and the text "User is not authorized to access the resource."
   7. Violation API information is the same data displayed within the dashboard
2. .env Information Leak
   1. <https://combine-1-elb-tap-e-ed11d741df7f5cd4.elb.us-east-1.amazonaws.com/tap/api/v1/users/.env>
   2. Navigating to this URL yields “User is not authorized to access the resource”
      1. This is a 401 unauthorized response; the finding appears to be invalid
3. .htaccess Information Leak
   1. <https://combine-1-elb-tap-e-ed11d741df7f5cd4.elb.us-east-1.amazonaws.com/tap/api/v1/users/.htaccess>
   2. Navigating to this URL yields “User is not authorized to access the resource”
      1. This is a 401 unauthorized response; the finding appears to be invalid.
4. Trace.axd Information leak
   1. GET <https://combine-1-elb-tap-e-ed11d741df7f5cd4.elb.us-east-1.amazonaws.com/tap/api/v1/users/trace.axd>
   2. Navigating to this URL yields “User is not authorized to access the resource”
      1. This is a 401 unauthorized response; the finding appears to be invalid.
5. User-Agent String Fuzzing
   1. Multiple user-agent strings were provided in GET requests to the site in an attempt to elicit a different response from the application.
   2. Any user-agent strings that alerted within ZAP shared the same response length with other user-agent strings sent to the same URI.
   3. The response header differed for each request as the timestamp and session-id were not the same, but this was the only difference.

# Appendix C: AWS Findings

The cloud assessment tool “Prowler” was executed against the Combine AWS production environment to test for compliance with AWS’ “Well Architected Framework”. The tool returned the following findings:

**High Criticality:**

1. **SEC01-BP02:** Root user should not be routinely used, have programmatic access and should have appropriate controls established.
   1. Affected resource:
      1. Root user: Multi-factor authentication (MFA) is not enabled for the root account

**Mitigation:** This is not controlled via the Combine application and therefore does not apply.

1. **SEC02-BP01:** Strong sign in mechanisms (such as MFA) should be used for all accounts.
   1. Affected resources:
      1. 776492542696: Password complexity, length and reuse need to be reviewed.
      2. The following resources do not use Multi-factor authentication:
         1. combine\_provisioning
         2. combine-security-assessor
         3. LuisReadOnlyAccessPaththinder

**Mitigation:** This is not controlled via the Combine application nor is it a part of the Combine baseline, therefore it does not apply.

1. **SEC02-BP02:** Temporary credentials should be used to eliminate risks from theft or disclosure.
   1. Affected resource:
      1. combine\_provisioning: User combine\_provisioning has not rotated access key 1 in over 90 days (682 days)

**Mitigation:** This is not controlled via the Combine application and therefore does not apply.

1. **SEC02-BP04:** Identities should be centrally managed
   1. Affected resources:
      1. The following resources could be affected by a cross-service confused deputy attack.
         1. Combine-EKS-Cluster
         2. Combine-EKS-Node
         3. Combine-I-Bastion
         4. Combine-I-CFN-CR-ConfigurationValue
         5. Combine-I-CFN-CR-ConfigureCombineFirewall
         6. Combine-I-Debug-Server
         7. Combine-I-Endpoints
         8. Combine-I-LogIngest
         9. Combine-I-LogListener
         10. Combine-I-Proxy
         11. Combine-I-Tap
         12. Combine-S-WLDEVELOPER-EC2
         13. Combine-TS-WLDEVELOPER-EC2
         14. LuisReadOnlyAccessTest

**Mitigation:** These changes will be evaluated prior to the 3.14 release.

1. **SEC03-BP01:** Access management should be clearly defined.
   1. Affected resource:
      1. i-00b4c9718c3da677f: IMDSv2 is disabled or not required.
         1. IMDSv2 is an enhanced version of the AWS Instance Metadata Service that improves security by requiring session-based tokens for accessing instance metadata and credentials. This helps mitigate risks such as Server-Side Request Forgery (SSRF) attacks by ensuring only authorized processes within an EC2 instance can retrieve sensitive information.

**Mitigation:** These changes will be evaluated prior to the 3.14 release. These changes will only be made if required in a customer environment.

1. **SEC04-BP01:** Service and application logging needs to be configured. Logs must be retained.
   1. Affected resources:
      1. 776492542696: No CloudTrail trails have a data event to record all S3 object-level API operations.

**Mitigation:** This is not applicable as it is not controlled by the Combine application. The customer shares responsibility for configuration.

* + 1. The following lambda functions are not recorded by CloudTrail.
       1. Combine\_CFN\_CF\_Configuration\_Value
       2. Combine\_CFN\_CF\_Configure\_Combine\_Firewall
       3. Combine\_Log\_Ingest
       4. Combine\_Log\_Listener\_Firewall

**Mitigation:** These changes will be evaluated prior to the 3.14 release.

* + 1. The following resources do not have access logs configured:
       1. Combine-1-ELB-Endpoints
       2. Combine-1-ELB-Tap-E
       3. Combine-1-ELB-Tap-I

**Mitigation:** These changes will be evaluated prior to the 3.14 release.

* + 1. The following resources have server access logging disabled
       1. cf-templates-1ueme6jh7wt3e-us-east-1
       2. combine-app-storage-776492542696
       3. combine-app-storage-776492542696-public
       4. combine-connection-logging-us-east-1-776492542696
       5. combine-devops-776492542696
       6. combine-devops-776492542696-us-east-1

**Mitigation:** This functionality can be enabled by customers if desired.

* + 1. vpc-042445bc36ec4511b: VPC Combine Flow logs are disabled.

**Mitigation:** These changes will be evaluated prior to the 3.14 release.

1. **SEC04-BP02:** Logs should be centrally collected, analyzed and managed
   1. Affected resources:
      1. 776492542696
         1. AWS Config recorder 776492542696 is disabled.
         2. No CloudTrail trails enabled with logging were found.
      2. vpc-042445bc36ec4511b: VPC Combine Flow logs are disabled.

**Mitigation:** This is not applicable as it is not controlled by the Combine application. The customer shares responsibility for configuration.

1. **SEC05-BP01:** Network segments should exist to restrict access only to necessary resources (ex: internet access, broader access within architecture etc.)
   1. Affected resources:
      1. All VPC endpoints listed can be accessed from non-trusted accounts:
         1. vpce-03492d36b0d2941aa
         2. vpce-0388bcb8177ab50bc
         3. vpce-07ffb13b2ec06bb9e
         4. vpce-0f2c7418733cb3d50

**Mitigation:** These endpoints were manually created and are not a part of the sequoia baseline.

1. **SEC05-BP02:** Configure network segments appropriately; all access between the internet and various internal subnets requires proper configuration.
   1. Affected resources:
      1. acl-0e3497a8b874acd2c: Port 22 is open to the internet
      2. The following resources have bucket ACLs and MFA Delete disabled:
         1. cf-templates-1ueme6jh7wt3e-us-east-1
         2. combine-app-storage-776492542696
         3. combine-app-storage-776492542696-public
         4. combine-devops-776492542696
      3. The following resources have MFA delete disabled:
         1. combine-connection-logging-us-east-1-776492542696
         2. combine-devops-776492542696-us-east-1

**Mitigation:** These are necessary settings for the environment; these settings will not be changed.

1. **SEC06-BP01:** Frequent scanning and patching for vulnerabilities needs to occur.
   1. Affected resources:
      1. i-00b4c9718c3da677f: IMDSv2 is disabled or not required.
      2. i-03b14bacecc04b262c
         1. internet facing IP of 52.70.28.12
         2. Internet facing Instance Profile arn:aws:iam::776492542696:instance-profile/Combine-I-Bastion
   2. **Mitigation:** Software will be deployed at the latest version; however, it is recommended as a best practice for the customer to conduct scans within their environment post-deployment.
2. **SEC08-BP02:** Enforce encryption at rest
   1. Affected resources:
      1. The following resources do not have AWS KMS keys associated
         1. /aws/eks/combine-test/cluster
         2. /aws/lambda/Combine\_CFN\_CF\_Configuration\_Value
         3. /aws/lambda/Combine\_CFN\_CF\_Configure\_Combine\_Firewall
         4. /aws/lambda/Combine\_Log\_Ingest
         5. /aws/lambda/Combine\_Log\_Listener\_Firewall
         6. /aws/lambda/Combine\_Log\_Listener\_Proxy
         7. /aws/lambda/Combine\_Log\_Listener\_Proxy\_FlowLogs
         8. Combine\_Log\_Group\_Endpoint
         9. Combine\_Log\_Group\_Firewall
         10. Combine\_Log\_Group\_Proxy\_Flow\_Logs
         11. Combine\_Log\_Group\_TAP
         12. Test

**Mitigation:** These changes will be evaluated prior to the 3.14 release.

* + 1. 776492542696: EBS Default Encryption is not activated.

**Mitigation:** Combine supports this as an option for customers that desire to use it.

* + 1. vol-0b089897f788c5663: EBS Snapshot vol-0b089897f788c5663 is unencrypted.

**Mitigation:** Combine supports this as an option for customers that desire to use it.

1. **SEC09-BP02:** Enforce encryption in transit
   1. Affected resources:
      1. The following resources do not have a bucket policy, allowing HTTP requests:
         1. cf-templates-1ueme6jh7wt3e-us-east-1
         2. combine-app-storage-776492542696
         3. combine-app-storage-776492542696-public
         4. combine-devops-776492542696
         5. combine-devops-776492542696-us-east-1
      2. Combine-1-ELB-Endpoints
         1. ELBv2 ALB Combine-1-ELB-Endpoints has non-encrypted listeners.
         2. ELBv2 Combine-1-ELB-Endpoints has listeners with insecure SSL protocols or ciphers (ELBSecurityPolicy-2016-08).
      3. combine-connection-logging-us-east-1-776492542696: allows requests over insecure transport in the bucket policy.

**Mitigation:** These changes will be evaluated prior to the 3.14 release.

1. **SEC10-BP01:** Identify key personnel and external resources
   1. Affected resource:
      1. 776492542696: AWS Support Access policy is not attached to any role.

**Mitigation:** This is not within the scope of control of the Combine application.

**Medium Criticality:**

1. **SEC01-BP06:** Automated testing should exist to validate all security controls continuously
   1. Affected resources:
      1. The following resources are not managed by a system manager:
         1. i-00b4c9718c3da677f
         2. i-03b14bacecc04b262
         3. i-0607f91570755b627
         4. i-0ad524f043beb0e17

**Mitigation:** System manager is not utilized by Combine. No planned fix at this time.

1. **SEC02-BP05:** Audit and rotate credentials periodically
   1. Affected resources:
      1. The following resources have rotation disabled:
         1. combine/configuration/certificates/ca/root/password
         2. combine/configuration/certificates/ca/signer/password
         3. combine/configuration/integrations/email/credentials/key
         4. combine/configuration/integrations/email/credentials/key/secret
      2. combine\_provisioning: Access key 1 has not been rotated in over 90 days (682 days)

**Mitigation:** Rotating credentials (including Certificate Authority) is too impactful on functionality of the environment. No planned fix at this time.

1. **SEC04-BP03:** Automate response to events; automated responses reduce human error and effort
   1. Affected resources:
      1. 776492542696: No CloudTrail trails enabled with logging were found.
      2. vpc-042445bc36ec4511b: VPC Combine Flow logs are disabled.

**Mitigation:** Won’t fix. Configuration is a shared responsibility with the customer.

1. **SEC05-BP03:** Automate network protections; AWS WAF can automatically block requests originating from IP addresses associated with known threat actors
   1. Affected resources:
      1. acl-0e3497a8b874acd2c
         1. Network ACL has every port open to the Internet.
         2. Network ACL has Microsoft RDP port 3389 open to the Internet.
         3. Network ACL has SSH port 22 open to the Internet.
      2. Combine-1-ELB-Endpoints
         1. ELBv2 ALB does not have desync mitigation mode set as strictest and is not dropping invalid header fields.
         2. ELBv2 ALB is not protected by WAF Web ACL.
      3. The following security groups are not being used:
         1. sg-003f396388ec4b071
         2. sg-0e51c21d8d0a02581
      4. (Customer has optional to provide customer managed security group) sg-00793fb4dc23681ff: Port 22 is open to the internet

**Mitigation:** These changes will be evaluated prior to the 3.14 release.

1. **SEC06-BP04:** Automate compute protection; this can help protect against human error, reduce attack surface and better manage resources.
   1. Affected resources:
      1. None of the following resources are managed by Systems Manager:
         1. i-00b4c9718c3da677f
         2. i-03b14bacecc04b262
         3. i-0607f91570755b627
         4. i-0ad524f043beb0e17

**Mitigation:** System manager is not utilized by Combine. No planned fix at this time.

**Low Criticality:**

1. **SEC02-BP06:** Leverage user groups and attributes. User and group attributes can help manage security requirements and permissions.
   1. Affected resources:
      1. combine\_provisioning/Combine-Provisioning
         1. User combine\_provisioning has the policy Combine-Provisioning attached.
      2. combine\_provisioning/Combine-Provisioning-EC2
         1. User combine\_provisioning has the policy Combine-Provisioning-EC2 attached.
      3. The following resources allow for privilege escalation with a large variety of actions (see the Well\_Architected\_Framework\_Results.xlsx attachment for all actions)
         1. Combine-Provisioning
         2. SPolicyCombineWLDEVELOPER
         3. TSPolicyCombineWLDEVELOPER

**Mitigation:** These changes fall outside the Combine application baseline and will not be fixed. These findings are not applicable.

1. **SEC03-BP06:** Manage access based on lifecycle. Users should be removed when they leave the organization and services like AWS Resource Access Manager can map users to resources as they are moved in and out of groups.
   1. Affected resources:
      1. 776492542696: Password expiration is not set.
      2. The following log groups have less than a 365 day log retention; they are set to 7 days:
         1. Combine\_Log\_Group\_Endpoint
         2. Combine\_Log\_Group\_Firewall
         3. Combine\_Log\_Group\_TAP

**Mitigation:** End users have the flexibility to set the retention period to their preferred duration. These logs generate a high volume of data and are primarily used for troubleshooting. By default, they will not be stored for 365 days.

1. **SEC03-BP07:** Analyze public and cross-account access; ensure that resources with public access are continuously monitored.
   1. Affected resources:
      1. 776492542696: ‘Block Public Access’ is not configured for this account
      2. i-03b14bacecc04b262: Instance has a Public IP: 52.70.28.12 (ec2-52-70-28-12.compute-1.amazonaws.com)

**Mitigation:** Combine does not utilize active scanning; no fix is planned at this time.

1. **SEC04-BP04:** Implement actionable security events that are sent to the team
   1. Affected resources:
      1. 776492542696
         1. GuardDuty is not enabled.
         2. No CloudWatch log groups found with metric filters or alarms associated.
      2. Security Hub: Security hub is not enabled

**Mitigation:** Combine does not use GuardDuty or Security Hub, as there is no technical requirement for these tools in a purely developmental environment. However, customers are free to implement these services if they find them suitable for their needs. There is no planned fix at this time.

1. **SEC05-BP04:** Implement inspection and protection at each layer.
   1. Affected resources:
      1. 776492542696
      2. vpc-042445bc36ec4511b

**Mitigation:** There is no technical requirement for these tools in a purely developmental environment. However, customers are free to implement these services if they find them suitable for their needs. There is no planned fix at this time.

1. **SEC06-BP05:** Enable people to perform actions at a distance
   1. Affected resources:
      1. The following systems are not managed by Systems Manager
         1. i-00b4c9718c3da677f
         2. i-03b14bacecc04b262
         3. i-0607f91570755b627
         4. i-0ad524f043beb0e17

**Mitigation:** System manager is not utilized by Combine. There is no planned fix at this time.

1. **SEC08-BP04:** Enforce access control to include encryption and versioning.
   1. Affected resources:
      1. The following S3 buckets have versioning disabled:
         1. cf-templates-1ueme6jh7wt3e-us-east-1
         2. combine-app-storage-776492542696
         3. combine-app-storage-776492542696-public
         4. combine-connection-logging-us-east-1-776492542696
         5. combine-devops-776492542696
         6. combine-devops-776492542696-us-east-1

**Mitigation:** These changes will be evaluated prior to the 3.14 release.

* + 1. The following resources are not encrypted
       1. Combine-Topic-Health-Monitor
       2. Combine-Topic-Violations
       3. Dynamodb

**Mitigation:** Customer has the option to enable encryption on these resources.

1. (Will evaluate for 3.14) SEC09-BP04: Authenticate network communications; enable VPC Combine flow logs
   1. Affected resource: vpc-042445bc36ec4511b

**Mitigation:** These changes will be evaluated prior to the 3.14 release.