Endida External Pen Test Service

ENDIDA
NEXT GENERATION CYBER DEFENCE

Sample Penetration Test Report

Prepared for Endida Ltd

Friday, 18 August 2023

Table of contents

1.2. Impact Summary

The pentest identified critical impacts that require immediate attention. These impacts represent critical vulnerabilities that can be leveraged by an attacker to compromise your network.

Critical Infrastructure Compromise (5)

Compromised 5 critical applications or devices

- Gitlab application at 18.221.8.100:80
- Jenkins application at 3.140.148.113:8083
- F5 Tmos application at 20.55.74.97:8443
- Vmware Horizon application at 3.133.93.223:443
- Admin privileges on compromised host 20.55.74.97 (f5.site01.h3airange.io) hosting critical applications (F5 Tmos)

Perimeter Breach (5)

Compromised 5 hosts via 6 separate attack vectors

- Host 3.133.93.223 (ec2-3-133-93-223.us-east-2.compute.amazonaws.com)
- Host 20.55.74.97 (f5.site01.h3airange.io)
- Host 3.140.148.113 (ec2-3-140-148-113.us-east-2.compute.amazonaws.com)
- Host 3.12.117.97 (ec2-3-12-117-97.us-east-2.compute.amazonaws.com)
- Host 3.136.39.26 (ec2-3-136-39-26.us-east-2.compute.amazonaws.com)

AWS User Role Compromise (1)

Compromised 1 user/role

- AWS Role h3aicloud-s3-full-access

Brand Compromise (2)

Compromised 2 subdomains via 3 separate attack vectors

- Subdomain doodle.site01.h3airange.io
- Application Unknown

Sensitive Data Exposure (6)

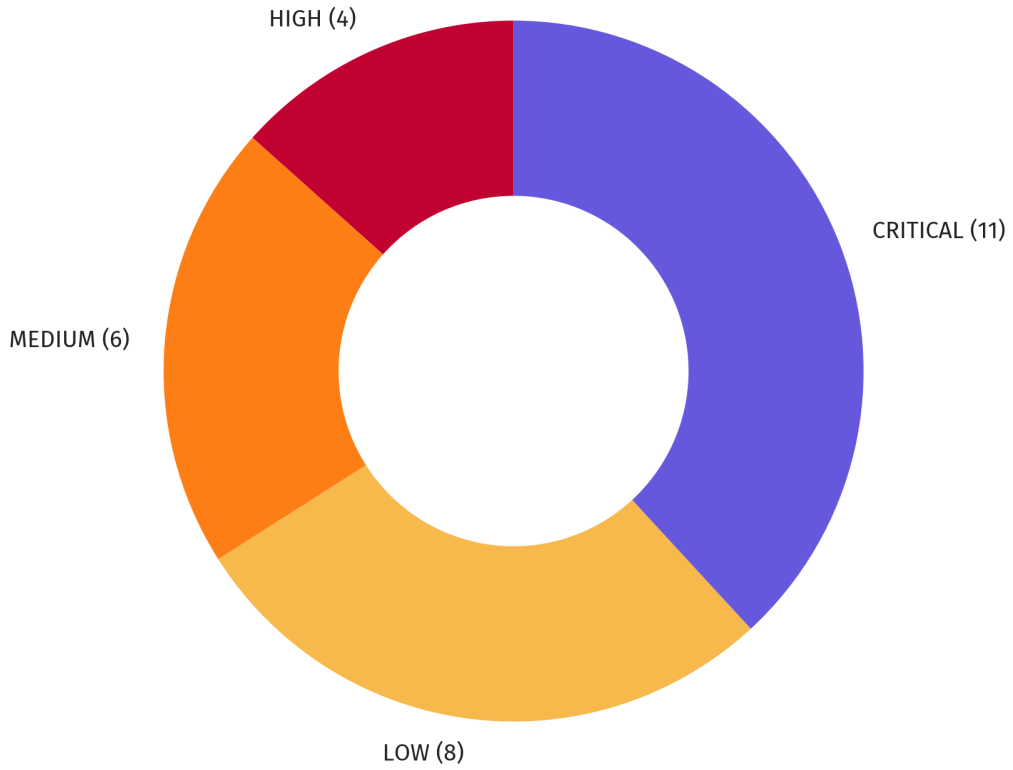
Compromised sensitive data on 6 stores

The top 5 are listed below.

- GitLab repo Test_truffle in account kbuch
- GitHub repo fakegit in account kbuch
- GitLab repo sensitive2 in account h3th4N
- GitLab repo fakegit2 in account kbuch
- GitLab repo secret_test in account kbuch

1.3. Weaknesses & Mitigations

The pentest identified CRITICAL degrees of risk within the target network, including **23 confirmed weaknesses** and **6 potential weaknesses.** These risks allow an attacker to steal data, disrupt operations, and cause financial or reputational loss.



Weaknesses by Severity

The following weaknesses were identified as having the highest degree of risk. Each weakness includes recommended mitigations and remediations.

The top 5 are listed below.

1. CRITICAL Apache Airflow Experimental API Authentication Bypass Vulnerability **(CVE-2020-13927, affecting 1 host)**

   Mitigations:

   In the Airflow configuration file, under [api] set the "auth_backend" value to "Airflow.api.auth.backend.deny_all". From Airflow 1.10.11 on this is the default behavior.

2. CRITICAL Apache Airflow Authorization Bypass Vulnerability **(CVE-2020-17526, affecting 1 host)**

   Mitigations:

   Update to Apache Airflow version >= 1.10.14.

   In the Airflow configuration file, under [webserver] set the "secret_key" value to a non-default value, preferably a long randomly-generated string.

3. CRITICAL F5 BIG-IP iControl REST Remote Command Execution Vulnerability **(CVE-2022-1388, affecting 1 host)**

   Mitigations:

   Apply all updates and patch to the latest vendor-supported version.

   If updating is not possible, follow the mitigations in the F5 Security Advisory.

4. CRITICAL JBoss Application Server HTTP Invoker Remote Code Execution Vulnerability **(H3-2021-0047, affecting 1 host)**

   Mitigations:

   Refer to your product vendor's guidance to disable the HTTP invoker endpoints.

   Follow the guidance below from SAS and IBM to disable the HTTP invoker endpoints. Ensure the /invoker/JMXInvokerServlet and /invoker/EJBInvokerServlet URLs are not accessible after the application server is restarted.

5. CRITICAL Gitlab GraphQL API Unauthenticated User Enumeration **(CVE-2021-4191, affecting 1 host)**

   Mitigations:

   Update Gitlab version to >= 14.6.6, 14.7.5, or 14.8.3

2. Findings

2.1. Impact Details

2.1.1. Critical Infrastructure Compromise (5)

Compromised 5 critical applications or devices

Critical infrastructure consists of key devices and applications that provide attackers a privileged position in the network from which they can access a wealth of sensitive data and launch further attacks.

Severity: CRITICAL

Host	Paths
Gitlab application at 18.221.8.100:80	• Gitlab Static Passwords For Users Registered with OmniAuth (CVE-2022-1162)
Jenkins application at 3.140.148.113:8083	• Unauthenticated Access to the Jenkins Script Console (H3-2020-0021)
F5 Tmos application at 20.55.74.97:8443	• F5 BIG-IP iControl REST Remote Command Execution Vulnerability (CVE-2022-1388)
Vmware Horizon application at 3.133.93.223:443	• Apache Log4j2 Remote Code Execution Vulnerability (CVE-2021-44228)
Admin privileges on compromised host 20.55.74.97 (f5.site01.h3airange.io) hosting critical applications (F5 Tmos)	• F5 BIG-IP iControl REST Remote Command Execution Vulnerability (CVE-2022-1388) affecting Web service at 20.55.74.97:8443

2.1.2. Perimeter Breach (5)

Compromised 5 hosts via 6 separate attack vectors

Perimeter breach can lead to attackers gaining access to your internal network from the public internet.

Severity: CRITICAL

Host	Paths
Host 3.133.93.223 (ec2-3-133-93-223.us-east-2.compute.amazonaws.com)	• Apache Log4j2 Remote Code Execution Vulnerability (CVE-2021-44228) affecting Web service at 3.133.93.223:443
Host 20.55.74.97 (f5.site01.h3airange.io)	• F5 BIG-IP iControl REST Remote Command Execution Vulnerability (CVE-2022-1388) affecting Web service at 20.55.74.97:8443
Host 3.140.148.113 (ec2-3-140-148-113.us-east-2.compute.amazonaws.com)	• Unauthenticated Access to the Jenkins Script Console (H3-2020-0021) affecting Web service at 3.140.148.113:8083 • Apache Airflow DAG Injection Remote Code Execution Vulnerability (CVE-2020-11978) affecting Web service at 3.140.148.113:80
Host 3.12.117.97 (ec2-3-12-117-97.us-east-2.compute.amazonaws.com)	• Apache Log4j2 Remote Code Execution Vulnerability (CVE-2021-44228) affecting Web service at 3.12.117.97:9200
Host 3.136.39.26 (ec2-3-136-39-26.us-east-2.compute.amazonaws.com)	• JBoss Application Server HTTP Invoker Remote Code Execution Vulnerability (H3-2021-0047) affecting Web service at 3.136.39.26:8081

2.1.3. AWS User Role Compromise (1)

Compromised 1 user/role

Once an AWS user or role is compromised, anything that user or role has access to including cloud resources, cloud services, and data should be considered compromised.

Severity: CRITICAL

Host	Paths
AWS Role h3aicloud-s3-full-access	• AWS Role h3aicloud-s3-full-access in account 132794086470

2.1.4. Brand Compromise (2)

Compromised 2 subdomains via 3 separate attack vectors

Brand compromise covers ways in which an attacker can harm your company's reputation by, for instance, defacing the company's website, hosting malware off the company's domain, or carrying out phishing attacks that appear to originate from the company.

Severity: HIGH

Host	Paths
Subdomain doodle.site01.h3airange.io	• Subdomain Takeover (H3-2021-0002) of doodle.site01.h3airange.io
Application Unknown	• Web Application Cross Site Scripting Vulnerability (H3-2022-0001) affecting application Unknown • Web Application Cross Site Scripting Vulnerability (H3-2022-0001) affecting application Unknown

2.1.5. Sensitive Data Exposure (6)

Compromised sensitive data on 6 stores

Sensitive data exposures can be used by attackers to obtain user credentials, PII (Personally Identifiable Information), financial account data, and other business-critical information to further exploit or gain profit.

Severity: HIGH

Host	Paths
GitLab repo Test_truffle in account kbuch	• Sensitive findings discovered in GitLab repo Test_truffle
GitHub repo fakegit in account kbuch	• Sensitive findings discovered in GitHub repo fakegit
GitLab repo sensitive2 in account h3th4N	• Sensitive findings discovered in GitLab repo sensitive2
GitLab repo fakegit2 in account kbuch	• Sensitive findings discovered in GitLab repo fakegit2
GitLab repo secret_test in account kbuch	• Sensitive findings discovered in GitLab repo secret_test
GitLab repo sensitive in account h3th4N	• Sensitive findings discovered in GitLab repo sensitive

2.2. Weakness Summary

The pentest identified CRITICAL degrees of risk within the target network, including **23 confirmed weaknesses** (with proof-of-exploit provided) and **6 potential weaknesses**.

2.2.1. Confirmed Weaknesses

Count	First Seen	Name	Weakness Id	Type	Severity
1	03:33PM	Apache Airflow Experimental API Authentication Bypass Vulnerability	CVE-2020-13927	VULNERABILITY	CRITICAL
1	03:32PM	Apache Airflow Authorization Bypass Vulnerability	CVE-2020-17526	VULNERABILITY	CRITICAL
1	03:32PM	F5 BIG-IP iControl REST Remote Command Execution Vulnerability	CVE-2022-1388	VULNERABILITY	CRITICAL
1	03:38PM	JBoss Application Server HTTP Invoker Remote Code Execution Vulnerability	H3-2021-0047	SECURITY_MISCONFIGURATION	CRITICAL
1	03:32PM	Gitlab GraphQL API Unauthenticated User Enumeration	CVE-2021-4191	VULNERABILITY	CRITICAL
3	03:39PM	Apache Log4j2 Remote Code Execution Vulnerability	CVE-2021-44228	VULNERABILITY	CRITICAL
1	03:32PM	Gitlab Static Passwords For Users Registered with OmniAuth	CVE-2022-1162	VULNERABILITY	CRITICAL
1	03:37PM	Unauthenticated Access to the Jenkins Script Console	H3-2020-0021	SECURITY_MISCONFIGURATION	CRITICAL
1	03:32PM	Apache Airflow DAG Injection Remote Code Execution Vulnerability	CVE-2020-11978	VULNERABILITY	CRITICAL
1	03:41PM	Apache mod_proxy Server-Side Request Forgery Vulnerability	CVE-2021-40438	VULNERABILITY	CRITICAL
1	03:38PM	AWS Instance Metadata Service v1 Exposed	H3-2021-0040	SECURITY_MISCONFIGURATION	CRITICAL
1	03:41PM	Grafana Directory Traversal Vulnerability	CVE-2021-43798	VULNERABILITY	HIGH
1	03:31PM	Subdomain Takeover	H3-2021-0002	SECURITY_MISCONFIGURATION	HIGH
2	03:43PM	Web Application Cross Site Scripting Vulnerability	H3-2022-0001	VULNERABILITY	HIGH
6	03:27PM	Public Access to Git Repository	H3-2021-0031	SECURITY_MISCONFIGURATION	HIGH
1	03:34PM	Unauthenticated Access to Elasticsearch	H3-2021-0036	SECURITY_MISCONFIGURATION	MEDIUM
1	03:41PM	Apache Solr Server-Side Request Forgery Vulnerability	CVE-2021-27905	VULNERABILITY	MEDIUM
1	03:40PM	Weak or Default Credentials - Web Applications	H3-2021-0021	CREDENTIALS	MEDIUM
1	03:41PM	Unauthenticated Access to Apache Solr	H3-2022-0028	SECURITY_MISCONFIGURATION	MEDIUM
1	03:39PM	Unauthenticated Access to Jenkins People Directory	H3-2022-0033	SECURITY_MISCONFIGURATION	MEDIUM
1	03:43PM	Apache Tomcat Example Scripts Exposed	H3-2022-0047	SECURITY_MISCONFIGURATION	MEDIUM
1	03:43PM	IIS web.config File Exposure	H3-2022-0049	SECURITY_MISCONFIGURATION	LOW
1	03:39PM	Web Directory Listing	H3-2022-0069	SECURITY_MISCONFIGURATION	LOW

2.2.2. Potential Weaknesses

Count	First Seen	Name	Weakness Id	Type	Severity
1	03:34PM	Remote Desktop Protocol (RDP) Port Exposed to the Internet	H3-2022-0003	SECURITY_MISCONFIGURATION	LOW
10	03:34PM	Secure Socket Shell (SSH) Port Exposed to the Internet	H3-2022-0005	SECURITY_MISCONFIGURATION	LOW
1	03:34PM	Risky Port Exposed to the Internet	H3-2022-0010	SECURITY_MISCONFIGURATION	LOW
1	03:30PM	Dangling DNS Record	H3-2021-0024	SECURITY_MISCONFIGURATION	LOW
2	03:38PM	Expired SSL/TLS Certificate	H3-2021-0025	SECURITY_MISCONFIGURATION	LOW
4	03:33PM	Public Self-Signed Certificate	H3-2021-0026	SECURITY_MISCONFIGURATION	LOW

2.3. Weakness Details

2.3.1. CVE-2020-13927: Apache Airflow Experimental API Authentication Bypass Vulnerability

Severity: CRITICAL

Description:

The previous default setting for Airflow's Experimental API was to allow all API requests without authentication, but this poses security risks to users who miss this fact. From Airflow 1.10.11 the default has been changed to deny all requests by default and is documented at https://airflow.apache.org/docs/1.10.11/security.html#api-authentication. Note this change fixes it for new installs but existing users need to change their config to default `[api]auth_backend = airflow.api.auth.backend.deny_all` as mentioned in the Updating Guide: https://github.com/apache/airflow/blob/1.10.11/UPDATING.md#experimental-api-will-deny-all-request-by-default

Impact: UNAUTHORIZED ACCESS INFORMATION DISCLOSURE

Unauthorized attackers can access the Airflow experimental API endpoints to read potentially sensitive data and chain with other vulnerabilities.

Mitigations:

- In the Airflow configuration file, under [api] set the " auth_backend" value to "Airflow.api.auth.backend.deny_all". From Airflow 1.10.11 on this is the default behavior.

References:

- CVE-2020-13927 @ https://nvd.nist.gov/vuln/detail/CVE-2020-13927
- Vendor Advisory @ https://lists.apache.org/thread/mq1bpqf3ztg1nhyc5qbrjobfrzttwx1d

Affected Applications:

Name	VHost	IP	Port	Severity
apache airflow	target-host3.site01.h3airange.io	3.140.148.113	tcp/80	CRITICAL

Related Credentials & Resources:

First Seen	Proof	Username	Role	Source	IP	Port	Service Type	Name	Permissions	Total Resources
03:39PM	Yes	admin	APPLICATION_USER	Default Login	3.136.39.26	tcp/8081	Web			1
03:35PM	No			Anonymous	3.136.39.26	tcp/8081	Web			5
03:31PM	No			Anonymous	3.133.93.223	tcp/443	Web			3
03:37PM	No			Anonymous	3.136.39.26	tcp/8081	Web			2
03:36PM	No			Anonymous	13.59.33.147	tcp/9090	Web			1
03:38PM	No			Anonymous	3.128.1.61	tcp/8983	Web			1
03:35PM	No			Anonymous	13.59.33.147	tcp/9090	Web			1
03:31PM	No			Anonymous	3.140.148.113	tcp/80	Web			1
03:31PM	No			Anonymous	3.140.148.113	tcp/80	Web			1

2.3.2. CVE-2020-17526: Apache Airflow Authorization Bypass Vulnerability

Severity: CRITICAL

Description:

Incorrect Session Validation in Apache Airflow Webserver versions prior to 1.10.14 with default config allows a malicious airflow user on site A where they log in normally, to access unauthorized Airflow Webserver on Site B through the session from Site A. This does not affect users who have changed the default value for `[webserver] secret_key` config.

Impact: UNAUTHORIZED ACCESS INFORMATION DISCLOSURE

Attackers can gain administrative access to the vulnerable application without authentication.

Mitigations:

- Update to Apache Airflow version >= 1.10.14.
- In the Airflow configuration file, under [webserver] set the " secret_key" value to a non-default value, preferably a long randomly-generated string.

References:

- CVE-2020-17526 @ https://nvd.nist.gov/vuln/detail/CVE-2020-17526
- Vendor Advisory @ https://lists.apache.org/thread/rrp5r6jfcjfjf32dbqs96zm7qbtho2ro

Affected Applications:

Name	VHost	IP	Port	Severity
apache airflow	target-host3.site01.h3airange.io	3.140.148.113	tcp/80	CRITICAL

Related Credentials & Resources:

First Seen	Proof	Username	Role	Source	IP	Port	Service Type	Name	Permissions	Total Resources
03:31PM	No			Anonymous	3.140.148.113	tcp/80	Web			1
03:31PM	No			Anonymous	3.140.148.113	tcp/80	Web			1

2.3.3. CVE-2022-1388: F5 BIG-IP iControl REST Remote Command Execution Vulnerability

Severity: CRITICAL

Description:

On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all 12.1.x and 11.6.x versions, undisclosed requests may bypass iControl REST authentication. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated

Impact: REMOTE CODE EXECUTION UNAUTHORIZED ACCESS PRIVILEGE ESCALATION

Unauthenticated attackers with access to the F5 BIG-IP iControl REST interface can gain complete control of the vulnerable BIG-IP host.

Mitigations:

- Apply all updates and patch to the latest vendor-supported version.
- If updating is not possible, follow the mitigations in the F5 Security Advisory.

References:

- CVE-2022-1388 @ https://nvd.nist.gov/vuln/detail/CVE-2022-1388
- F5 Security Advisories @ https://support.f5.com/csp/article/K23605346

Affected Applications:

Name	VHost	IP	Port	Severity
f5 tmos		20.55.74.97	tcp/8443	CRITICAL

Related Credentials & Resources:

First Seen	Proof	Username	Role	Source	IP	Port	Service Type	Name	Permissions	Total Resources
03:31PM	No			Anonymous	20.55.74.97	tcp/8443	Web			2

2.3.4. H3-2021-0047: JBoss Application Server HTTP Invoker Remote Code Execution Vulnerability

Severity: CRITICAL

Description:

The JBoss server allows unauthenticated users to access the /invoker/JMXInvokerServlet and /invoker/EJBInvokerServlet endpoints. This is a default configuration is JBoss 4.x, 5.x, and 6.x.

Impact: REMOTE CODE EXECUTION UNAUTHORIZED ACCESS

This misconfiguration permits unauthenticated remote attackers to run arbitary commands on the vulnerable host by submitting crafted serialized Java payloads to the /invoker/JMXInvokerServlet or /invoker/EJBInvokerServlet URLs.

Mitigations:

- Refer to your product vendor' s guidance to disable the HTTP invoker endpoints.
- Follow the guidance below from SAS and IBM to disable the HTTP invoker endpoints. Ensure the /invoker/JMXInvokerServlet and /invoker/EJBInvokerServlet URLs are not accessible after the application server is restarted.

References:

- JexBoss - JBoss Verify and Exploitation Tool @ https://github.com/joaomatosf/jexboss
- CISA Analysis Report (AR18-312A): JexBoss – JBoss Verify and EXploitation Tool @ https://www.cisa.gov/uscert/ncas/analysis-reports/AR18-312A
- FoxGlove Security: What Do WebLogic, WebSphere, JBoss, Jenkins, OpenNMS, and Your Application Have in Common? @ https://foxglovesecurity.com/2015/11/06/what-do-weblogic-websphere-jboss-jenkins-opennms-and-your-application-have-in-common-this-vulnerability/#jboss
- SAS Guidance: Removing the JMX Console and the EJBInvokerServlet and JMXInvokerServlet applications from the JBoss application server @ http://support.sas.com/kb/53/977.html
- IBM: JBoss Security Remediation Guidance @ https://www.ibm.com/docs/en/SSHEB3_3.7/pdfs_wiki/Jboss_Security_Remediation.pdf

Affected Applications:

Name	VHost	IP	Port	Severity
redhat jboss	target-host5.site01.h3airange.io	3.136.39.26	tcp/8081	CRITICAL

Related Credentials & Resources:

First Seen	Proof	Username	Role	Source	IP	Port	Service Type	Name	Permissions	Total Resources
03:39PM	Yes	admin	APPLICATION_USER	Default Login	3.136.39.26	tcp/8081	Web			1
03:35PM	No			Anonymous	3.136.39.26	tcp/8081	Web			5
03:31PM	No			Anonymous	3.133.93.223	tcp/443	Web			3

First Seen	Proof	Username	Role	Source	IP	Port	Service Type	Name	Permissions	Total Resources
03:37PM	No			Anonymous	3.136.39.26	tcp/8081	Web			2
03:36PM	No			Anonymous	13.59.33.147	tcp/9090	Web			1
03:38PM	No			Anonymous	3.128.1.61	tcp/8983	Web			1
03:37PM	No			Anonymous	3.128.1.61	tcp/8081	Web			1
03:35PM	No			Anonymous	3.128.1.61	tcp/8081	Web			1
03:35PM	No			Anonymous	13.59.33.147	tcp/9090	Web			1
03:36PM	No			Anonymous	3.128.1.61	tcp/8081	Web			1
03:31PM	No			Anonymous	3.140.148.113	tcp/80	Web			1
03:31PM	No			Anonymous	3.140.148.113	tcp/80	Web			1

2.3.5. CVE-2021-4191: Gitlab GraphQL API Unauthenticated User Enumeration

Severity: CRITICAL

Description:

An issue has been discovered in GitLab CE/EE affecting versions 13.0 to 14.6.5, 14.7 to 14.7.4, and 14.8 to 14.8.2. Private GitLab instances with restricted sign-ups may be vulnerable to user enumeration to unauthenticated users through the GraphQL API.

Impact: UNAUTHORIZED ACCESS INFORMATION DISCLOSURE

This vulnerability enables an attacker to enumerate Gitlab users. This provides a starting point for attackers to launch brute force, password guessing, and credential stuffing attacks.

Mitigations:

- Update Gitlab version to >= 14.6.6, 14.7.5, or 14.8.3

References:

- CVE-2021-4191 @ https://nvd.nist.gov/vuln/detail/CVE-2021-4191
- Gitlab Critical Security Release: 14.8.2, 14.7.4, and 14.6.5 @ https://about.gitlab.com/releases/2022/02/25/critical-security-release-gitlab-14-8-2-released/#unauthenticated-user-enumeration-on-graphql-api

Affected Applications:

Name	VHost	IP	Port	Severity
gitlab	gitlab.site01.h3airange.io	18.221.8.100	tcp/80	CRITICAL

Related Credentials & Resources:

First Seen	Proof	Username	Role	Source	IP	Port	Service Type	Name	Permissions	Total Resources
03:33PM	Yes	user	APPLICATION_USER	CVE_2022_1162	18.221.8.100	tcp/80	Web			1
03:33PM	No			Anonymous	18.221.8.100	tcp/80	Web			1
03:33PM	No			Anonymous	18.221.8.100	tcp/80	Web			1
03:32PM	No			Anonymous	18.221.8.100	tcp/80	Web			1

2.3.6. CVE-2021-44228: Apache Log4j2 Remote Code Execution Vulnerability Log4Shell

Severity: CRITICAL

Description:

Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default. From version 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been completely removed. Note that this vulnerability is specific to log4j-core and does not affect log4net, log4cxx, or other Apache Logging Services projects.

Impact: INFORMATION DISCLOSURE UNAUTHORIZED ACCESS REMOTE CODE EXECUTION

The severity of this vulnerability depends on the target application and configuration. In the worst case, this vulnerability permits unauthenticated attackers to gain control of the vulnerable host and execute arbitrary commands on it.

Mitigations:

- For applications running with Java 8 or later, follow the guidance of the vendor of the affected application to update the Apache log4j2 library to version >= 2.17.1. Restart the affected application.
- For applications running with Java 7, follow the guidance of the vendor of the affected application to update the Apache log4j2 library to version >= 2.12.4. Restart the affected application.
- For applications running with Java 6, follow the guidance of the vendor of the affected application to update the Apache log4j2 library to version >= 2.3.2. Restart the affected application.
- Remove the JndiLookup class from the classpath of the vulnerable application using the command: zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class. Restart the affected application.

References:

- CISA Advisory @ https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance
- Compilation of Vendor Advisories @ https://gist.github.com/SwitHak/b66db3a06c2955a9cb71a8718970c592
- Cheat Sheet Reference Guide @ https://www.techsolvency.com/story-so-far/cve-2021-44228-log4j-log4shell/

- Apache Log4j2 Release Notes @ https://logging.apache.org/log4j/2.x/security.html

- CVE-2021-44228 @ https://nvd.nist.gov/vuln/detail/CVE-2021-44228

Affected Applications:

Name	VHost	IP	Port	Severity
vmware horizon	horizon.site01.h3airange.io	3.133.93.223	tcp/443	CRITICAL
elasticsearch	target-host6.site01.h3airange.io	3.12.117.97	tcp/9200	CRITICAL
apache solr		3.128.1.61	tcp/8983	HIGH

Related Credentials & Resources:

First Seen	Proof	Username	Role	Source	IP	Port	Service Type	Name	Permissions	Total Resources
03:39PM	Yes	admin	APPLICATION_USER	Default Login	3.136.39.26	tcp/8081	Web			1
03:33PM	Yes	user	APPLICATION_USER	CVE_2022_1162	18.221.8.100	tcp/80	Web			1
03:37PM	No			Anonymous	3.140.148.113	tcp/8083	Web			15
03:35PM	No			Anonymous	3.136.39.26	tcp/8081	Web			5
03:31PM	No			Anonymous	3.133.93.223	tcp/443	Web			3
03:37PM	No			Anonymous	3.136.39.26	tcp/8081	Web			2
03:36PM	No			Anonymous	13.59.33.147	tcp/9090	Web			1
03:38PM	No			Anonymous	3.128.1.61	tcp/8983	Web			1
03:37PM	No			Anonymous	3.128.1.61	tcp/8081	Web			1
03:33PM	No			Anonymous	18.221.8.100	tcp/80	Web			1
03:35PM	No			Anonymous	3.128.1.61	tcp/8081	Web			1
03:38PM	No			Anonymous	3.12.117.97	tcp/9200	Web			1
03:35PM	No			Anonymous	13.59.33.147	tcp/9090	Web			1
03:36PM	No			Anonymous	3.128.1.61	tcp/8081	Web			1
03:33PM	No			Anonymous	18.221.8.100	tcp/80	Web			1
03:31PM	No			Anonymous	3.140.148.113	tcp/80	Web			1
03:32PM	No			Anonymous	18.221.8.100	tcp/80	Web			1
03:31PM	No			Anonymous	3.140.148.113	tcp/80	Web			1
03:36PM	No			Anonymous	3.12.117.97	tcp/9200	Web			1

2.3.7. CVE-2022-1162: Gitlab Static Passwords For Users Registered with OmniAuth

Severity: CRITICAL

Description:

A hardcoded password was set for accounts registered using an OmniAuth provider (e.g. OAuth, LDAP, SAML) in GitLab CE/EE versions 14.7 prior to 14.7.7, 14.8 prior to 14.8.5, and 14.9 prior to 14.9.2 allowing attackers to potentially take over accounts

Impact: UNAUTHORIZED ACCESS INFORMATION DISCLOSURE

This vulnerability enables an attacker to login to Gitlab as a legitimate user and perform any actions with the privileges of that user.

Mitigations:

- Update Gitlab version to >= 14.9.3, 14.7.8, or 14.8.6

References:

- CVE-2022-1162 @ https://nvd.nist.gov/vuln/detail/CVE-2022-1162
- Gitlab Critical Security Release: 14.9.2, 14.8.5, and 14.7.7 @ https://about.gitlab.com/releases/2022/03/31/critical-security-release-gitlab-14-9-2-released/#static-passwords-inadvertently-set-during-omniauth-based-registration

Affected Applications:

Name	VHost	IP	Port	Severity
gitlab	gitlab.site01.h3airange.io	18.221.8.100	tcp/80	CRITICAL

Related Credentials & Resources:

First Seen	Proof	Username	Role	Source	IP	Port	Service Type	Name	Permissions	Total Resources
03:33PM	Yes	user	APPLICATION_USER	CVE_2022_1162	18.221.8.100	tcp/80	Web			1
03:32PM	Yes	user	APPLICATION_USER	CVE_2022_1162	18.221.8.100	tcp/80	Web			0
03:33PM	No			Anonymous	18.221.8.100	tcp/80	Web			1
03:33PM	No			Anonymous	18.221.8.100	tcp/80	Web			1
03:32PM	No			Anonymous	18.221.8.100	tcp/80	Web			1

2.3.8. H3-2020-0021: Unauthenticated Access to the Jenkins Script Console

Severity: CRITICAL

Description:

The Jenkins server exposes the script console to unauthenticated users.

Impact: REMOTE CODE EXECUTION INFORMATION DISCLOSURE UNAUTHORIZED ACCESS PRIVILEGE ESCALATION

Attackers can use the Jenkins script console to execute arbitrary commands on the Jenkins host and to gain shell access. Attackers can gain access to credentials stored in Jenkins or other confidential data.

Mitigations:

- Restrict access to the script console to administrative users. Disable unauthenticated script console access in the Global Security Configuration section of the admin interface.

References:

- Securing Jenkins @ https://www.jenkins.io/doc/book/system-administration/security/
- Jenkins - Script-Console Java Execution (Metasploit) @ https://www.exploit-db.com/exploits/24272

Affected Applications:

Name	VHost	IP	Port	Severity
jenkins	target-host3.site01.h3airange.io	3.140.148.113	tcp/8083	CRITICAL

Related Credentials & Resources:

First Seen	Proof	Username	Role	Source	IP	Port	Service Type	Name	Permissions	Total Resources
03:37PM	No			Anonymous	3.140.148.113	tcp/8083	Web			15

Related Potential Credentials:

First Seen	User	Key Type	Password	Hash	Source	Domain	Service Type
03:37PM	baduser	cleartext	b*********d		Plaintext/Hash Dump		
03:37PM	jsmith	cleartext	S*********!		Plaintext/Hash Dump		
03:37PM	user	cleartext	p*******		Plaintext/Hash Dump		

2.3.9. CVE-2020-11978: Apache Airflow DAG Injection Remote Code Execution Vulnerability

Severity: CRITICAL

Description:

An issue was found in Apache Airflow versions 1.10.10 and below. A remote code/command injection vulnerability was discovered in one of the example DAGs shipped with Airflow which would allow any authenticated user to run arbitrary commands as the user running airflow worker/scheduler (depending on the executor in use). If you already have examples disabled by setting load_examples=False in the config then you are not vulnerable.

Impact: REMOTE CODE EXECUTION UNAUTHORIZED ACCESS INFORMATION DISCLOSURE

Attackers can execute arbitrary code on the machine hosting the vulnerable application.

Mitigations:

- Update to Apache Airflow version >= 1.10.11.
- In the Airflow configuration file, under [core] set " load_examples" to be "False".

References:

- CVE-2020-11978 @ https://nvd.nist.gov/vuln/detail/CVE-2020-11978
- Vendor Advisory @ https://lists.apache.org/thread/cn57zwylxsnzjyjztwqxpmly0x9q5ljx

Affected Applications:

Name	VHost	IP	Port	Severity
apache airflow	target-host3.site01.h3airange.io	3.140.148.113	tcp/80	CRITICAL

Related Credentials & Resources:

First Seen	Proof	Username	Role	Source	IP	Port	Service Type	Name	Permissions	Total Resources
03:31PM	No			Anonymous	3.140.148.113	tcp/80	Web			1
03:31PM	No			Anonymous	3.140.148.113	tcp/80	Web			1

2.3.10. CVE-2021-40438: Apache mod_proxy Server-Side Request Forgery Vulnerability

Severity: CRITICAL

Description:

A crafted request uri-path can cause mod_proxy to forward the request to an origin server choosen by the remote user. This issue affects Apache HTTP Server 2.4.48 and earlier.

Impact: INFORMATION DISCLOSURE UNAUTHORIZED ACCESS REMOTE CODE EXECUTION

This vulnerability allows a remote, unauthenticated attacker to make the httpd server forward requests to an arbitrary server. The attacker could get, modify, or delete resources on other services that may be behind a firewall and inaccessible otherwise. The impact of this flaw varies based on what services and resources are available on the httpd network.

Mitigations:

- This vulnerability affects Apache HTTP Server 2.4.48 and earlier. Upgrade the product to the latest version.

References:

- What is SSRF? @ https://portswigger.net/web-security/ssrf
- Apache 2.4 Vulnerabilities @ https://httpd.apache.org/security/vulnerabilities_24.html
- CVE-2021-40438 @ https://nvd.nist.gov/vuln/detail/CVE-2021-40438

Affected Applications:

Name	VHost	IP	Port	Severity
apache httpd_server	jenkins.site01.h3airange.io	3.128.1.61	tcp/8081	CRITICAL

Related Credentials & Resources:

First Seen	Proof	Username	Role	Source	IP	Port	Service Type	Name	Permissions	Total Resources
03:32PM	No			Anonymous	18.221.8.100	tcp/ 8080	Web			96
03:39PM	Yes	admin	APPLICATION_USER	Default Login	3.136.39.26	tcp/ 8081	Web			1
03:38PM	Yes	h3aicloud-s3-full-access	AWS_ROLE	SSRF	N/A		AWS STS		read	0
03:40PM	Yes	h3aicloud-s3-full-access	AWS_ROLE	SSRF	N/A		AWS ELASTICBEANSTALK		read	0
03:40PM	Yes	h3aicloud-s3-full-access	AWS_ROLE	SSRF	N/A		AWS ROUTE53		read	0
03:40PM	Yes	h3aicloud-s3-full-access	AWS_ROLE	SSRF	N/A		AWS S3		read	0
03:37PM	No			Anonymous	3.140.148.113	tcp/ 8083	Web			15
03:35PM	No			Anonymous	3.136.39.26	tcp/ 8081	Web			5
03:37PM	No			Anonymous	3.136.39.26	tcp/ 8081	Web			2
03:32PM	No			Anonymous	18.221.8.100	tcp/ 8080	Web			2
03:32PM	No			Anonymous	18.221.8.100	tcp/ 8080	Web			2
03:37PM	No			Anonymous	3.128.1.61	tcp/ 8081	Web			1
03:35PM	No			Anonymous	3.128.1.61	tcp/ 8081	Web			1
03:38PM	No			Anonymous	3.12.117.97	tcp/ 9200	Web			1
03:36PM	No			Anonymous	3.128.1.61	tcp/ 8081	Web			1
03:35PM	No			Anonymous	3.136.39.26	tcp/ 3000	Web			1
03:36PM	No			Anonymous	3.12.117.97	tcp/ 9200	Web			1

2.3.11. H3-2021-0040: AWS Instance Metadata Service v1 Exposed

Severity: CRITICAL

Description:

The AWS Instance Metadata Service runs on a special internal link-local IP 169.254.169.154 and hosts configuration for the instance. Metadata Service v1 (IMDSv1) is vulnerable to exploitation by remote attackers in combination with other vulnerabilities such as server-side request forgery (SSRF).

Impact: INFORMATION DISCLOSURE UNAUTHORIZED ACCESS

An attacker can obtain AWS access keys from the Metadata Service. An attacker can use these access keys to access AWS cloud services, data, and resources. The breadth of impact depends on the permissions configured with the instance.

Mitigations:

- Determine if the instance needs to utilize the Instance Metadata Service (IMDS) and disable it if possible.
- Reconfigure the IMDS service for the affected instance to utilize IMDS Version 2.

References:

- Using IMDSv2 @ https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/configuring-instance-metadata-service.html

Affected Hosts:

IP	Host Name	Operating System	Severity
3.128.1.61	ec2-3-128-1-61.us-east-2.compute.amazonaws.com	Ubuntu Linux 20.04	CRITICAL

Related Credentials & Resources:

First Seen	Proof	Username	Role	Source	IP	Port	Service Type	Name	Permissions	Total Resources
03:38PM	Yes	h3aicloud-s3-full-access	AWS_ROLE	SSRF	N/A		AWS STS		read	0
03:40PM	Yes	h3aicloud-s3-full-access	AWS_ROLE	SSRF	N/A		AWS ELASTICBEANSTALK		read	0
03:40PM	Yes	h3aicloud-s3-full-access	AWS_ROLE	SSRF	N/A		AWS ROUTE53		read	0
03:40PM	Yes	h3aicloud-s3-full-access	AWS_ROLE	SSRF	N/A		AWS S3		read	0
03:37PM	No			Anonymous	3.128.1.61	tcp/8081	Web			1
03:35PM	No			Anonymous	3.128.1.61	tcp/8081	Web			1
03:36PM	No			Anonymous	3.128.1.61	tcp/8081	Web			1

2.3.12. CVE-2021-43798: Grafana Directory Traversal Vulnerability

Severity: HIGH

Description:

Grafana is an open-source platform for monitoring and observability. Grafana versions 8.0.0-beta1 through 8.3.0 (except for patched versions) iss vulnerable to directory traversal, allowing access to local files. The vulnerable URL path is: `<grafana_host_url>/public/plugins//`, where is the plugin ID for any installed plugin. At no time has Grafana Cloud been vulnerable. Users are advised to upgrade to patched versions 8.0.7, 8.1.8, 8.2.7, or 8.3.1. The GitHub Security Advisory contains more information about vulnerable URL paths, mitigation, and the disclosure timeline.

Impact: UNAUTHORIZED ACCESS INFORMATION DISCLOSURE

This vulnerability allows a remote, unauthenticated attacker to access local files through a vulnerable URL path. These local files may contain sensitive data such as credentials.

Mitigations:

- Upgrade to versions 8.3.1, 8.2.7, 8.1.8, 8.0.7 or higher.

References:

- An update on 0day CVE-2021-43798: Grafana directory traversal @ https://grafana.com/blog/2021/12/08/an-update-on-0day-cve-2021-43798-grafana-directory-traversal/
- CVE-2021-43798 @ https://nvd.nist.gov/vuln/detail/CVE-2021-43798

Affected Applications:

Name	VHost	IP	Port	Severity
grafana		3.136.39.26	tcp/3000	HIGH

Related Credentials & Resources:

First Seen	Proof	Username	Role	Source	IP	Port	Service Type	Name	Permissions	Total Resources
03:32PM	No			Anonymous	18.221.8.100	tcp/8080	Web			96
03:37PM	No			Anonymous	3.140.148.113	tcp/8083	Web			15
03:32PM	No			Anonymous	18.221.8.100	tcp/8080	Web			2
03:32PM	No			Anonymous	18.221.8.100	tcp/8080	Web			2
03:37PM	No			Anonymous	3.128.1.61	tcp/8081	Web			1
03:35PM	No			Anonymous	3.128.1.61	tcp/8081	Web			1
03:36PM	No			Anonymous	3.128.1.61	tcp/8081	Web			1
03:35PM	No			Anonymous	3.136.39.26	tcp/3000	Web			1

2.3.13. H3-2021-0002: Subdomain Takeover

Severity: HIGH

Description:

The DNS record for a subdomain has a CNAME record that points to another subdomain that is not in use. Attackers may be able to claim the subdomain that is the CNAME for this subdomain.

Impact: DEFACEMENT IMPERSONATION

By taking over a legitimate looking company domain, attackers can trick users through phishing campaigns, attempt to steal user cookies and passwords, deface the company web site and damage the company brand.

Mitigations:

- If the subdomain is not in use, remove the stale DNS record for it.
- If the subdomain is in use, reclaim the subdomain that is the CNAME, or set a new valid CNAME for this subdomain.

References:

- Subdomain Takeovers: Thoughts on Risk @ https://0xpatrik.com/subdomain-takeover/
- Prevent Dangling DNS Entries and Avoid Subdomain Takeover @ https://docs.microsoft.com/en-us/azure/security/fundamentals/subdomain-takeover

Affected External Domains:

Domain	CNAME	IP Addresses	Severity
doodle.site01.h3airange.io	11285521401250.s3-website.us-east-2.amazonaws.com	52.219.102.168	HIGH

2.3.14. H3-2022-0001: Web Application Cross Site Scripting Vulnerability

Severity: HIGH

Description:

Cross-site scripting is an client-side attack method that injects malicious code such as JavaScript or iFrames into a vulnerable web application to exploit users of the application.

Impact: UNAUTHORIZED ACCESS INFORMATION DISCLOSURE DEFACEMENT IMPERSONATION

This attack permits unauthenticated remote attackers to gain the privileges of exploited users of the web application. The extent of impact depends on the permissions that exploited users have within the application.

Mitigations:

- Refer to your product vendor' s guidance to upgrade the vulnerable web application to a patched version.

References:

- Cross Site Scripting (XSS) @ https://owasp.org/www-community/attacks/xss/

Affected Applications:

Name	VHost	IP	Port	Severity
unknown	target-host6.site01.h3airange.io	3.12.117.97	tcp/800	HIGH
unknown	target-host6.site01.h3airange.io	3.12.117.97	tcp/4443	HIGH

Related Credentials & Resources:

First Seen	Proof	Username	Role	Source	IP	Port	Service Type	Name	Permissions	Total Resources
03:32PM	No			Anonymous	18.221.8.100	tcp/8080	Web			96
03:38PM	No			Anonymous	3.140.148.113	tcp/8082	Web			7
03:36PM	No			Anonymous	3.12.117.97	tcp/4443	Web			4
03:35PM	No			Anonymous	3.12.117.97	tcp/800	Web			3
03:32PM	No			Anonymous	18.221.8.100	tcp/8080	Web			2
03:32PM	No			Anonymous	18.221.8.100	tcp/8080	Web			2
03:37PM	No			Anonymous	3.12.117.97	tcp/800	Web			1
03:38PM	No			Anonymous	3.12.117.97	tcp/4443	Web			1

2.3.15. H3-2021-0031: Public Access to Git Repository

Severity: HIGH

Description:

A Git repository that your company may own is publicly accessible.

Impact: INFORMATION DISCLOSURE

Attackers may be able to identify sensitive data in the source code stored in the repository.

Mitigations:

- Confirm the repository should be publicly accessible, and if not remove public access and only allow authorized users to access the repository.
- Review and regularly audit the source code stored in the repository for sensitive data that should not be publicly exposed.

References:

- Security Best Practices for GitHub Enterprise Server @ https://github.blog/2019-12-05-security-best-practices-for-github-enterprise-server/
- Security Best Practices for Git Users @ https://resources.infosecinstitute.com/topic/security-best-practices-for-git-users/
- 10 GitHub Security Best Practices @ https://snyk.io/blog/ten-git-hub-security-best-practices/

- Removing sensitive data from a repository @ https://docs.github.com/en/github/authenticating-to-github/removing-sensitive-data-from-a-repository

Affected Repositories:

Name	Service Type	IP	Port	Severity
sensitive	GitLab: h3th4N			HIGH
secret_test	GitLab: kbuch			HIGH
fakegit2	GitLab: kbuch			HIGH
fakegit	GitHub: kbuch			HIGH
sensitive2	GitLab: h3th4N			HIGH
Test_truffle	GitLab: kbuch			HIGH

Related Credentials & Resources:

First Seen	Proof	Username	Role	Source	IP	Port	Service Type	Name	Permissions	Total Resources
03:31PM	No			Anonymous	N/A			secret_test	read	2
03:30PM	No			Anonymous	N/A			sensitive	read	10
03:31PM	No			Anonymous	N/A			fakegit2	read	2
03:31PM	No			Anonymous	N/A			Test_truffle	read	2
03:30PM	No			Anonymous	N/A			sensitive2	read	5
03:30PM	No			Anonymous	N/A			fakegit	read	4

2.3.16. H3-2021-0036: Unauthenticated Access to Elasticsearch

Severity: MEDIUM

Description:

Elasticsearch is a distributed search engine, commonly used for log aggregation and analysis. Unauthenticated access to Elasticsearch allows attackers to retrieve and potentially alter data in the cluster.

Impact: UNAUTHORIZED ACCESS INFORMATION DISCLOSURE FILE UPLOAD

Attackers can access sensitive data stored in the Elasticsearch cluster, such as plain-text passwords, operational intelligence, and business-critical information. Attackers with write access can tamper with data and reconfigure the cluster.

Mitigations:

- Require authentication to access the Elasticsearch cluster. Enabling xpack.security.enabled=True in the configuration file will disable anonymous access.

References:

- Set up Minimal Security for Elasticsearch @ https://www.elastic.co/guide/en/elasticsearch/reference/current/security-minimal-setup.html

Affected Applications:

Name	VHost	IP	Port	Severity
elasticsearch	target-host6.site01.h3airange.io	3.12.117.97	tcp/9200	MEDIUM

Related Credentials & Resources:

First Seen	Proof	Username	Role	Source	IP	Port	Service Type	Name	Permissions	Total Resources
03:38PM	No			Anonymous	3.12.117.97	tcp/9200	Web			1
03:36PM	No			Anonymous	3.12.117.97	tcp/9200	Web			1

2.3.17. CVE-2021-27905: Apache Solr Server-Side Request Forgery Vulnerability

Severity: MEDIUM

Description:

The ReplicationHandler (normally registered at "/replication" under a Solr core) in Apache Solr has a "masterUrl" (also "leaderUrl" alias) parameter that is used to designate another ReplicationHandler on another Solr core to replicate index data into the local core. To prevent a SSRF vulnerability, Solr ought to check these parameters against a similar configuration it uses for the "shards" parameter. Prior to this bug getting fixed, it did not. This problem affects essentially all Solr versions prior to it getting fixed in 8.8.2.

Impact: INFORMATION DISCLOSURE UNAUTHORIZED ACCESS REMOTE CODE EXECUTION

This vulnerability allows a remote, unauthenticated attacker to make the Apache Solr server forward requests to an arbitrary server. The attacker could get, modify, or delete resources on other services that may be behind a firewall and inaccessible otherwise. The impact of this flaw varies based on what services and resources are available on the Apache Solr network.

Mitigations:

- This vulnerability affects Apache Solr version 8.8.1 and earlier. Upgrade the product to the latest version.

References:

- What is SSRF? @ https://portswigger.net/web-security/ssrf
- Apache Solr Security News @ https://solr.apache.org/security.html
- CVE-2021-27905 @ https://nvd.nist.gov/vuln/detail/CVE-2021-27905

Affected Applications:

Name	VHost	IP	Port	Severity
apache solr		3.128.1.61	tcp/8983	MEDIUM

Related Credentials & Resources:

First Seen	Proof	Username	Role	Source	IP	Port	Service Type	Name	Permissions	Total Resources
03:39PM	Yes	admin	APPLICATION_USER	Default Login	3.136.39.26	tcp/8081	Web			1
03:35PM	No			Anonymous	3.136.39.26	tcp/8081	Web			5
03:31PM	No			Anonymous	3.133.93.223	tcp/443	Web			3
03:37PM	No			Anonymous	3.136.39.26	tcp/8081	Web			2
03:36PM	No			Anonymous	13.59.33.147	tcp/9090	Web			1
03:38PM	No			Anonymous	3.128.1.61	tcp/8983	Web			1
03:35PM	No			Anonymous	13.59.33.147	tcp/9090	Web			1
03:31PM	No			Anonymous	3.140.148.113	tcp/80	Web			1
03:31PM	No			Anonymous	3.140.148.113	tcp/80	Web			1

2.3.18. H3-2021-0021: Weak or Default Credentials - Web Applications

Severity: MEDIUM

Description:

Weak credentials include passwords that are easily obtained by password guessing, password spraying, or cracked using dictionary attacks. Default passwords are publicly known and obtainable by an attacker and provide immediate access to a system.

Impact: INFORMATION DISCLOSURE UNAUTHORIZED ACCESS

An attacker can openly maneuver throughout an environment and access information if a password is compromised.

Mitigations:

- Ensure a strong password policy is in place and users are properly trained on best practices. Consider the use of a password manager to store complex passwords where possible.
- Identify a configuration management process that ensures default credentials are changed before systems are deployed in a production environment.
- Implement multi-factor authentication where possible.

References:

- CWE-521: Weak Password Requirements @ https://cwe.mitre.org/data/definitions/521.html
- T1110: Brute Force @ https://attack.mitre.org/techniques/T1110/

Affected Credentials:

Username	Role	Source	Service Type	IP	Port	Severity
admin	APPLICATION_USER	Default Login	Web	3.136.39.26	tcp/8081	MEDIUM

Related Credentials & Resources:

First Seen	Proof	Username	Role	Source	IP	Port	Service Type	Name	Permissions	Total Resources
03:40PM	Yes	admin	APPLICATION_USER	Default Login	3.136.39.26	tcp/8081	Web			0
03:39PM	Yes	admin	APPLICATION_USER	Default Login	3.136.39.26	tcp/8081	Web			1
03:39PM	Yes	admin	APPLICATION_USER	Default Login	3.136.39.26	tcp/8081	Web			0
03:35PM	No			Anonymous	3.136.39.26	tcp/8081	Web			5
03:37PM	No			Anonymous	3.136.39.26	tcp/8081	Web			2

2.3.19. H3-2022-0028: Unauthenticated Access to Apache Solr

Severity: MEDIUM

Description:

Solr is highly reliable, scalable and fault tolerant, providing distributed indexing, replication and load-balanced querying, automated failover and recovery, centralized configuration and more.

Impact: UNAUTHORIZED ACCESS INFORMATION DISCLOSURE

Depending on permissions, an attacker could get, modify, or delete resources that may be inaccessible otherwise. The impact of this flaw varies based on what services and resources are available on the network.

Mitigations:

- Disable anonymous access. Administrators should configure their deployments following guides listed in references.

References:

- Basic Authentication Plugin @ https://solr.apache.org/guide/7_6/basic-authentication-plugin.html
- Securing Solr With Basic Authentication @ https://lucidworks.com/post/securing-solr-basic-auth-permission-rules/

Affected Applications:

Name	VHost	IP	Port	Severity
apache solr		3.128.1.61	tcp/8983	MEDIUM

Related Credentials & Resources:

First Seen	Proof	Username	Role	Source	IP	Port	Service Type	Name	Permissions	Total Resources
03:39PM	Yes	admin	APPLICATION_USER	Default Login	3.136.39.26	tcp/8081	Web			1
03:35PM	No			Anonymous	3.136.39.26	tcp/8081	Web			5
03:31PM	No			Anonymous	3.133.93.223	tcp/443	Web			3
03:37PM	No			Anonymous	3.136.39.26	tcp/8081	Web			2
03:36PM	No			Anonymous	13.59.33.147	tcp/9090	Web			1

First Seen	Proof	Username	Role	Source	IP	Port	Service Type	Name	Permissions	Total Resources
03:38PM	No			Anonymous	3.128.1.61	tcp/8983	Web			1
03:35PM	No			Anonymous	13.59.33.147	tcp/9090	Web			1
03:31PM	No			Anonymous	3.140.148.113	tcp/80	Web			1
03:31PM	No			Anonymous	3.140.148.113	tcp/80	Web			1

2.3.20. H3-2022-0033: Unauthenticated Access to Jenkins People Directory

Severity: MEDIUM

Description:

The Jenkins People Directory requires no authentication.

Impact: UNAUTHORIZED ACCESS INFORMATION DISCLOSURE

An unauthenticated attacker can use the data available on this page to compile a list of known users to conduct further credential attacks with. Jenkins applications are likely targets of attackers due to the abundance of information and credentials stored on it.

Mitigations:

- Disable anonymous access. Administrators should configure their deployments following guides listed in references.

References:

- Managing Security @ https://www.jenkins.io/doc/book/security/managing-security/
- Access granted with Overall/Read @ https://www.jenkins.io/doc/book/security/access-control/permissions/#overall-read

Affected Applications:

Name	VHost	IP	Port	Severity
jenkins	target-host3.site01.h3airange.io	3.140.148.113	tcp/8083	MEDIUM

Related Credentials & Resources:

First Seen	Proof	Username	Role	Source	IP	Port	Service Type	Name	Permissions	Total Resources
03:32PM	No			Anonymous	18.221.8.100	tcp/8080	Web			96
03:37PM	No			Anonymous	3.140.148.113	tcp/8083	Web			15
03:32PM	No			Anonymous	18.221.8.100	tcp/8080	Web			2
03:32PM	No			Anonymous	18.221.8.100	tcp/8080	Web			2
03:37PM	No			Anonymous	3.128.1.61	tcp/8081	Web			1
03:35PM	No			Anonymous	3.128.1.61	tcp/8081	Web			1
03:38PM	No			Anonymous	3.12.117.97	tcp/9200	Web			1

First Seen	Proof	Username	Role	Source	IP	Port	Service Type	Name	Permissions	Total Resources
03:36PM	No			Anonymous	3.128.1.61	tcp/8081	Web			1
03:35PM	No			Anonymous	3.136.39.26	tcp/3000	Web			1
03:36PM	No			Anonymous	3.12.117.97	tcp/9200	Web			1

2.3.21. H3-2022-0047: Apache Tomcat Example Scripts Exposed

Severity: MEDIUM

Description:

Example scripts come with Apache Tomcat v4.x - v7.x by default

Impact: INFORMATION DISCLOSURE

These files can be used by attackers to gain information about the system. These scripts are also known to be vulnerable to cross site scripting (XSS) injection and may leak sensitive session information about users.

Mitigations:

- Restrict access to these files or remove them from the system.

References:

- Apache Tomcat vulnerabilities @ https://tomcat.apache.org/security-4.html

Affected Applications:

Name	VHost	IP	Port	Severity
apache tomcat	gitlab.site01.h3airange.io	18.221.8.100	tcp/8080	MEDIUM

Related Credentials & Resources:

First Seen	Proof	Username	Role	Source	IP	Port	Service Type	Name	Permissions	Total Resources
03:32PM	No			Anonymous	18.221.8.100	tcp/8080	Web			96
03:38PM	No			Anonymous	3.140.148.113	tcp/8082	Web			7
03:36PM	No			Anonymous	3.12.117.97	tcp/4443	Web			4
03:32PM	No			Anonymous	18.221.8.100	tcp/8080	Web			2
03:32PM	No			Anonymous	18.221.8.100	tcp/8080	Web			2
03:38PM	No			Anonymous	3.12.117.97	tcp/4443	Web			1

2.3.22. H3-2022-0049: IIS web.config File Exposure

Severity: LOW

Description:

The IIS server configuration file web.config is exposed.

Impact: INFORMATION DISCLOSURE

Having server configuration exposed supplies a lot of sensitive information which may help an attacker to prepare for an attack of the applications.

Mitigations:

- Restrict access to these files.

References:

- Web.config file exposed vulnerability @ https://community.spiceworks.com/topic/2295658-web-config-file-exposed-vulnerability

Affected Applications:

Name	VHost	IP	Port	Severity
microsoft iis	target-host3.site01.h3airange.io	3.140.148.113	tcp/8082	LOW

Related Credentials & Resources:

First Seen	Proof	Username	Role	Source	IP	Port	Service Type	Name	Permissions	Total Resources
03:32PM	No			Anonymous	18.221.8.100	tcp/8080	Web			96
03:38PM	No			Anonymous	3.140.148.113	tcp/8082	Web			7
03:36PM	No			Anonymous	3.12.117.97	tcp/4443	Web			4
03:32PM	No			Anonymous	18.221.8.100	tcp/8080	Web			2
03:32PM	No			Anonymous	18.221.8.100	tcp/8080	Web			2
03:38PM	No			Anonymous	3.12.117.97	tcp/4443	Web			1

2.3.23. H3-2022-0069: Web Directory Listing

Severity: LOW

Description:

Webservers with directory listing enabled can reveal files stored on the webserver that are not intended to be served as part of the web application.

Impact: UNAUTHORIZED ACCESS INFORMATION DISCLOSURE

Directory listings can enable an attacker to gain unauthorized access to sensitive information on the web server, such as source code, configuration files, keys, webserver data, and webserver backup files.

Mitigations:

- Disable directory listing on the web server.

References:

- CWE-552 @ https://cwe.mitre.org/data/definitions/552.html
- Disable directory listing in Apache @ https://www.simplified.guide/apache/disable-directory-listing
- Disable directory listing in nginx @ http://nginx.org/en/docs/http/ngx_http_autoindex_module.html
- Disable directory listing in IIS @ https://localcoder.org/disable-directory-listing-in-iis

Affected Applications:

Name	VHost	IP	Port	Severity
unknown	target-host3.site01.h3airange.io	3.140.148.113	tcp/4443	LOW

Related Credentials & Resources:

First Seen	Proof	Username	Role	Source	IP	Port	Service Type	Name	Permissions	Total Resources
03:38PM	No			Anonymous	3.140.148.113	tcp/4443	Web			19

2.3.24. H3-2022-0003: Remote Desktop Protocol (RDP) Port Exposed to the Internet

Severity: LOW

Description:

The RDP service is accessbble from the internet.

Impact: UNAUTHORIZED ACCESS

RDP exposure has been a leading source of company breaches over the last few years. Attackers can conduct credential attacks by utilizing passwords found from past data breaches and conduct password spray attacks. If successful, this gives attackers access to the internal network.

Mitigations:

- Use industry best practices for remote management, like implementing a VPN to allow remote users to access internal assets via an encrypted tunnel.
- If VPNs are not possible, ensure complex passwords are in use as well as multi-factor authentication.
- Limit access to remote management services on hosts to specific management hosts to reduce overall attack surface.

References:

- CSO Online @ https://www.csoonline.com/article/3542895/attacks-against-internet-exposed-rdp-servers-surging-during-covid-19-pandemic.html

Affected Services:

IP	Port	IANA Service Name	Product	Severity
3.133.93.223	tcp/3389	ms-wbt-server	Microsoft Terminal Services	LOW

Related Credentials & Resources:

First Seen	Proof	Username	Role	Source	IP	Port	Service Type	Name	Permissions	Total Resources
03:38PM	No			Anonymous	3.12.117.97	tcp/9200	Web			1
03:36PM	No			Anonymous	3.12.117.97	tcp/9200	Web			1

2.3.25. H3-2022-0005: Secure Socket Shell (SSH) Port Exposed to the Internet

Severity: LOW

Description:

The SSH service is accessible from the internet.

Impact: UNAUTHORIZED ACCESS

Attackers can leverage access to remote management services to gain an initial foothold in a company network. Attackers often gain access through credential attacks by obtaining passwords leaked in data breaches and by password spraying weak passwords.

Mitigations:

- Use industry best practices for remote management, like implementing a VPN to allow remote users to access internal assets via an encrypted tunnel.
- If VPNs are not possible, ensure SSH authentication is only possible with key-based authentication versus passwords.
- Limit access to remote management services on hosts to specific management hosts to reduce overall attack surface.

References:

- Securing OpenSSH @ https://wiki.centos.org/HowTos/Network/SecuringSSH
- Eight ways to protect SSH access on your system @ https://www.redhat.com/sysadmin/eight-ways-secure-ssh

Affected Services:

IP	Port	IANA Service Name	Product	Severity
3.12.117.97	tcp/22	ssh	OpenBSD OpenSSH 8.2p1 Ubuntu 4ubuntu0.3	LOW
3.128.1.61	tcp/22	ssh	OpenBSD OpenSSH 8.2p1 Ubuntu 4ubuntu0.3	LOW
3.130.245.239	tcp/22	ssh	OpenBSD OpenSSH 8.2p1 Ubuntu 4ubuntu0.3	LOW
3.135.128.226	tcp/22	ssh	OpenBSD OpenSSH 8.2p1 Ubuntu 4ubuntu0.3	LOW
3.136.39.26	tcp/22	ssh	OpenBSD OpenSSH 8.2p1 Ubuntu 4ubuntu0.3	LOW
3.140.148.113	tcp/22	ssh	OpenBSD OpenSSH 8.2p1 Ubuntu 4ubuntu0.3	LOW

IP	Port	IANA Service Name	Product	Severity
13.59.33.147	tcp/22	ssh	OpenBSD OpenSSH 8.2p1 Ubuntu 4ubuntu0.3	LOW
13.59.203.16	tcp/22	ssh	OpenBSD OpenSSH 8.2p1 Ubuntu 4ubuntu0.3	LOW
18.221.8.100	tcp/22	ssh	OpenBSD OpenSSH 8.2p1 Ubuntu 4ubuntu0.3	LOW
20.55.74.97	tcp/22	ssh	OpenBSD OpenSSH 7.4	LOW

Related Credentials & Resources:

First Seen	Proof	Username	Role	Source	IP	Port	Service Type	Name	Permissions	Total Resources
03:38PM	No			Anonymous	3.12.117.97	tcp/9200	Web			1
03:36PM	No			Anonymous	3.12.117.97	tcp/9200	Web			1

2.3.26. H3-2022-0010: Risky Port Exposed to the Internet

Severity: LOW

Description:

Ports that could allow for remote access to hardware, software or files and folder should not be publicly available on the internet.

Impact: UNAUTHORIZED ACCESS

Attackers could gain access to sensitive data or gain further access into a companies environment be it software or hardware.

Mitigations:

- Block all in-bound and out-bound traffic at the boundary of your network and only allow known source and destination ports to where they are needed to go according to company policy.

References:

Affected Services:

IP	Port	IANA Service Name	Product	Severity
3.133.93.223	tcp/389	ldap		LOW

Related Credentials & Resources:

First Seen	Proof	Username	Role	Source	IP	Port	Service Type	Name	Permissions	Total Resources
03:38PM	No			Anonymous	3.12.117.97	tcp/9200	Web			1
03:36PM	No			Anonymous	3.12.117.97	tcp/9200	Web			1

2.3.27. H3-2021-0024: Dangling DNS Record

Severity: LOW

Description:

The DNS record for a subdomain has a CNAME record that points to another subdomain that is not in use or does not resolve to an IP address.

Impact: DEFACEMENT IMPERSONATION

A dangling DNS record gives attackers an opportunity to attempt a subdomain takeover. By taking over a legitimate looking company domain, attackers can trick users through phishing campaigns, attempt to steal user cookies and passwords, deface the company web site and damage the company brand.

Mitigations:

- If the subdomain is not in use, remove the stale DNS record for it.
- If the subdomain is in use, set its CNAME record to a valid DNS hostname.

References:

- Subdomain Takeovers: Thoughts on Risk @ https://0xpatrik.com/subdomain-takeover/
- Prevent Dangling DNS Entries and Avoid Subdomain Takeover @ https://docs.microsoft.com/en-us/azure/security/fundamentals/subdomain-takeover

Affected External Domains:

Domain	CNAME	IP Addresses	Severity
doodle.site01.h3airange.io	11285521401250.s3-website.us-east-2.amazonaws.com	52.219.102.168	LOW

2.3.28. H3-2021-0025: Expired SSL/TLS Certificate

Severity: LOW

Description:

The SSL/TLS certificate has expired or is close to expiring.

Impact: IMPERSONATION

An expired certificate causes browser security warnings to appear when a user browses to the web site using the certificate. These warnings erode user trust in the web site and create alert fatigue. Attackers can take advantage of this by launching man-in-the-middle attacks using a fraudulent certificate and trick users into divulging confidential information. If the web site uses HTTP Strict Transport Security (HSTS) and has an expired certificate, users won't be able to browse to it at all.

Mitigations:

- Renew the certificate.
- If not in use, shut down the web site with the expired certificate.

References:

- Let's Encrypt @ https://letsencrypt.org/docs/
- Public Key Certificate @ https://en.wikipedia.org/wiki/Public_key_certificate
- HTTP Strict Transport Security @ https://https.cio.gov/hsts/

Affected Services:

IP	Port	IANA Service Name	Product	Severity
3.12.117.97	tcp/4443	https	Apache HTTPD, Moodle, Unknown	LOW
3.140.148.113	tcp/4443	https	Apache HTTPD 2.4.52, Unknown	LOW

2.3.29. H3-2021-0026: Public Self-Signed Certificate

Severity: LOW

Description:

The SSL/TLS certificate is self-signed.

Impact: IMPERSONATION

Self-signed certificates should not be used for public user-facing web sites. A self-signed certificate causes browser security warnings to appear when a user browses to the web site using the certificate. These warnings erode user trust in the web site and create alert fatigue. Attackers can take advantage of this by launching man-in-the-middle attacks using a fraudulent certificate and trick users into divulging confidential information. If the web site uses HTTP Strict Transport Security (HSTS) and has a self-signed certificate, users won't be able to browse to it at all.

Mitigations:

- Replace the self-signed certificate with a certificate signed by an official trusted Certificate Authority.
- Configure network access controls to prevent public access to the web site that is using the self-signed certificate.
- If not in use, shut down the web site with the self-signed certificate.

References:

- Let's Encrypt @ https://letsencrypt.org/docs/
- Self-Signed Certificate @ https://en.wikipedia.org/wiki/Self-signed_certificate
- HTTP Strict Transport Security @ https://https.cio.gov/hsts/

Affected Services:

IP	Port	IANA Service Name	Product	Severity
3.12.117.97	tcp/4443	https	Apache HTTPD, Moodle, Unknown	LOW
3.140.148.113	tcp/4443	https	Apache HTTPD 2.4.52, Unknown	LOW

IP	Port	IANA Service Name	Product	Severity
18.221.8.100	tcp/8443	rtsp		LOW
20.55.74.97	tcp/8443	https	Apache HTTPD, F5 Tmos	LOW

3. Appendices

3.1. Credentials

The pentest captured **3 confirmed credentials** (with proof-of-access) and **3 potential credentials**.

3.1.1. Confirmed Credentials

First Seen	Username	Type	Iana Svc Name	Source	IP Addr	Port	Product
03:38PM	h3aicloud-s3-full-access	AWS		SSRF			
03:39PM	admin	STANDARD	http	Default Login	3.136.39.26:8081	8081	Apache Tomcat/Coyote JSP Engine 1.1, Oracle Java Management Extensions, Red Hat JBoss AS, Redhat Jboss Enterprise Application Platform
03:32PM	user	STANDARD	http	CVE_2022_1162	18.221.8.100:80	80	GitLab, Igor Sysoev Nginx

3.1.2. Potential Credentials

First Seen	Username	Type	Iana Svc Name	Source	IP Addr	Port	Product
03:37PM	jsmith	STANDARD		Plaintext/ Hash Dump			
03:37PM	user	STANDARD		Plaintext/ Hash Dump			
03:37PM	baduser	STANDARD		Plaintext/ Hash Dump			

3.2. Hosts

The pentest discovered **18 hosts**.

3.2.1. In Scope Hosts

First Seen	Host Name	IP	OS	Weaknesses	Data Res	Creds	Services	Web
03:30PM	ec2-3-140-148-113.us-east-2.compute.amazonaws.com	3.140.148.113	Debian Linux, Ubuntu Linux 20.04	10	0	0	6	5
03:30PM	ec2-3-136-39-26.us-east-2.compute.amazonaws.com	3.136.39.26	Ubuntu Linux 20.04	4	0	1	3	4
03:30PM	f5.site01.h3airange.io	20.55.74.97	F5 Tmos	3	0	0	5	1
03:30PM	ec2-18-221-8-100.us-east-2.compute.amazonaws.com	18.221.8.100	Ubuntu Linux 20.04	5	0	1	4	10
03:30PM	ec2-3-128-1-61.us-east-2.compute.amazonaws.com	3.128.1.61	Ubuntu Linux 20.04	6	0	0	3	4
03:30PM	ec2-3-12-117-97.us-east-2.compute.amazonaws.com	3.12.117.97	Ubuntu Linux 20.04	6	0	0	4	6
03:30PM	ec2-3-133-93-223.us-east-2.compute.amazonaws.com	3.133.93.223	Microsoft Windows	3	0	0	10	1
03:30PM	ec2-13-59-33-147.us-east-2.compute.amazonaws.com	13.59.33.147	Debian Linux, Ubuntu Linux 20.04	1	0	0	2	2
03:30PM	ec2-3-130-245-239.us-east-2.compute.amazonaws.com	3.130.245.239	Ubuntu Linux 20.04	1	0	0	1	0
03:30PM	ec2-3-135-128-226.us-east-2.compute.amazonaws.com	3.135.128.226	Ubuntu Linux 20.04	1	0	0	1	0
03:30PM	ec2-13-59-203-16.us-east-2.compute.amazonaws.com	13.59.203.16	Ubuntu Linux 20.04	1	0	0	1	0

3.2.2. Out of Scope Hosts

First Seen	Host Name	IP	OS	Weaknesses	Data Res	Creds	Services	Web
03:30PM	ec2-3-133-186-163.us-east-2.compute.amazonaws.com	3.133.186.163		0	0	0	0	0
03:30PM	ec2-3-232-249-216.compute-1.amazonaws.com	3.232.249.216		0	0	0	0	0
03:30PM	s3-website.us-east-2.amazonaws.com	52.219.102.168		2	0	0	0	0
03:30PM	s3-website.us-east-2.amazonaws.com	52.219.105.124		0	0	0	0	0
03:30PM	s3-website.us-east-2.amazonaws.com	52.219.109.48		0	0	0	0	0
03:30PM	ec2-54-80-190-177.compute-1.amazonaws.com	54.80.190.177		0	0	0	0	0
03:30PM	226.16.197.104.bc.googleusercontent.com	104.197.16.226		0	0	0	0	0

3.3. Data Resources

The pentest discovered **25 data resources** on **19 stores** containing potentially sensitive information.

3.3.1. Git Repositories

Source	Account Name	Name	Clone Url	Forked	Sensitive Findings	Severity
GitLab	kbuch	Test_truffle	https://gitlab.com/kbuch/test_truffle.git		2	HIGH
GitHub	kbuch	fakegit	https://github.com/kbuch/fakegit.git		4	HIGH
GitLab	h3th4N	sensitive2	https://gitlab.com/h3th4n/h4x0r/sensitive2.git		5	HIGH
GitLab	kbuch	fakegit2	https://gitlab.com/kbuch/fakegit2.git		2	HIGH
GitLab	kbuch	secret_test	https://gitlab.com/kbuch/secret_test.git	true	2	HIGH
GitLab	h3th4N	sensitive	https://gitlab.com/h3th4n/sensitive.git		10	HIGH

3.3.2. S3 Buckets

Name	Service	Resources Count	Permissions	Severity
my-temp-mongo-backup-h3ai	AWS S3	0		INFO
h3airange-terraform-state-prod	AWS S3	0		INFO
225224209-836959327-135773468	AWS S3	0		INFO

Name	Service	Resources Count	Permissions	Severity
datadog-forwarder-range-forwarderbucket-aclho8mz62iu	AWS S3	0		INFO
h3aicloud-range-pritunl-mongodb-backup-dev	AWS S3	0		INFO
h3airange-terraform-state-dev	AWS S3	0		INFO
h3airange-vmdk-images	AWS S3	0		INFO
gd-range-s3	AWS S3	0		INFO
h3aicloud-tf-base-state	AWS S3	0		INFO
gdrange	AWS S3	0		INFO
testing-time-metadata-possibility	AWS S3	0		INFO
site01-vuln	AWS S3	0		INFO
h3aicloud-range-pritunl-mongodb-backup-prod	AWS S3	0		INFO

3.3.3. Databases

The pentest did not discover any Databases.

3.3.4. File Shares

The pentest did not discover any File Shares.

3.3.5. Docker Registries

The pentest did not discover any Docker Registries.

3.4. Web Resources & Certificates

The pentest crawled **188 web resources** on **33 web applications** and discovered **6 web certificates** containing potentially sensitive information.

3.4.1. Applications

First Seen	IP	Port	Product	Total Resources	Login Pages
03:31PM	18.221.8.100	tcp/8080	Apache Tomcat 10.0.21	96	2
03:31PM	3.140.148.113	tcp/4443	Apache HTTPD 2.4.52, Unknown	19	0
03:31PM	3.140.148.113	tcp/8083	Eclipse Jetty 9.4.43.v20210629, Jenkins	16	2
03:31PM	3.140.148.113	tcp/8082	Apache HTTPD 2.4.25, Drupal CMS, Microsoft Iis	7	2
03:31PM	3.136.39.26	tcp/8081	Apache Tomcat/Coyote JSP Engine 1.1, Oracle Java Management Extensions, Red Hat JBoss AS, Redhat Jboss Enterprise Application Platform	6	3
03:31PM	3.12.117.97	tcp/4443	Apache HTTPD, Moodle, Unknown	4	1
03:31PM	3.133.93.223	tcp/443	VMware Horizon	4	0
03:31PM	3.12.117.97	tcp/800	Apache HTTPD, Moodle, Unknown	3	1
03:31PM	3.136.39.26	tcp/8081	Apache Tomcat/Coyote JSP Engine 1.1, Oracle Java Management Extensions, Red Hat JBoss AS, Redhat Jboss Enterprise Application Platform	3	3
03:31PM	18.221.8.100	tcp/8080	Apache Tomcat 10.0.21	2	3
03:31PM	18.221.8.100	tcp/8080	Apache Tomcat 10.0.21	2	3
03:31PM	18.221.8.100	tcp/8443		2	1
03:31PM	20.55.74.97	tcp/8443	Apache HTTPD, F5 Tmos	2	1
03:31PM	3.128.1.61	tcp/8983	Apache Solr	2	0
03:31PM	3.136.39.26	tcp/3000	Grafana	2	0
03:31PM	3.12.117.97	tcp/4443	Apache HTTPD, Moodle, Unknown	1	0
03:31PM	3.12.117.97	tcp/9200	Elasticsearch REST API 5.6.0	1	0
03:31PM	3.12.117.97	tcp/9200	Elasticsearch REST API 5.6.0	1	0
03:31PM	18.221.8.100	tcp/80	GitLab, Igor Sysoev Nginx	1	2
03:31PM	18.221.8.100	tcp/80	GitLab, Igor Sysoev Nginx	1	2
03:31PM	18.221.8.100	tcp/80	GitLab, Igor Sysoev Nginx	1	1
03:31PM	18.221.8.100	tcp/80	GitLab, Igor Sysoev Nginx	1	1
03:31PM	18.221.8.100	tcp/8443		1	0
03:31PM	18.221.8.100	tcp/8443		1	0
03:31PM	3.128.1.61	tcp/8081	Apache Httpd Server 2.4, Edgecast CDN Httpd	1	0
03:31PM	3.128.1.61	tcp/8081	Apache Httpd Server 2.4, Edgecast CDN Httpd	1	0

First Seen	IP	Port	Product	Total Resources	Login Pages
03:31PM	3.128.1.61	tcp/8081	Apache Httpd Server 2.4, Edgecast CDN Httpd	1	0
03:31PM	3.136.39.26	tcp/8081	Apache Tomcat/Coyote JSP Engine 1.1, Oracle Java Management Extensions, Red Hat JBoss AS, Redhat Jboss Enterprise Application Platform	1	3
03:31PM	3.140.148.113	tcp/80	Apache Airflow, Igor Sysoev Nginx	1	2
03:31PM	3.140.148.113	tcp/80	Apache Airflow, Igor Sysoev Nginx	1	2
03:31PM	13.59.33.147	tcp/9090	Apache HTTPD 2.4.38, Wordpress	1	1
03:31PM	13.59.33.147	tcp/9090	Apache HTTPD 2.4.38, Wordpress	1	1
03:31PM	3.12.117.97	tcp/800	Apache HTTPD, Moodle, Unknown	1	0

3.4.2. Certificates

First Seen	IP	Port	Expiration	Issuer	Common Name	Signed?
03:36PM	3.133.93.223	443	06/5/24	horizon.h3airange.io (VMware, Inc.)	horizon.h3airange.io	No
03:37PM	3.133.93.223	8443	06/5/24	horizon.h3airange.io (VMware, Inc.)	horizon.h3airange.io	No
03:38PM	3.12.117.97	4443	11/12/22	example.com	example.com	No
03:39PM	3.140.148.113	4443	07/27/21	Internet Widgits Pty Ltd from AU		No
03:33PM	20.55.74.97	8443	05/28/32	localhost.localdomain (MyCompany from --)	localhost.localdomain	No
03:33PM	18.221.8.100	8443	05/21/32	keycloak.site01.h3airange.io (Internet Widgits Pty Ltd from US)	keycloak.site01.h3airange.io	No

3.5. Services

The pentest scanned **40 services** during the operation.

First Seen	IP	Port	Iana Service Name	Product	Severity
03:31PM	3.140.148.113	tcp/80	http	Apache Airflow, Igor Sysoev Nginx	CRITICAL
03:31PM	3.136.39.26	tcp/8081	http	Apache Tomcat/Coyote JSP Engine 1.1, Oracle Java Management Extensions, Red Hat JBoss AS, Redhat Jboss Enterprise Application Platform	CRITICAL
03:31PM	20.55.74.97	tcp/8443	https	Apache HTTPD, F5 Tmos	CRITICAL
03:31PM	3.140.148.113	tcp/8083	http	Eclipse Jetty 9.4.43.v20210629, Jenkins	CRITICAL

First Seen	IP	Port	Iana Service Name	Product	Severity
03:31PM	18.221.8.100	tcp/80	http	GitLab, Igor Sysoev Nginx	CRITICAL
03:31PM	3.12.117.97	tcp/9200	http	Elasticsearch REST API 5.6.0	CRITICAL
03:31PM	3.128.1.61	tcp/8983	http	Apache Solr	HIGH
03:31PM	3.133.93.223	tcp/443	https	VMware Horizon	HIGH
03:31PM	3.128.1.61	tcp/8081	http	Apache Httpd Server 2.4, Edgecast CDN Httpd	HIGH
03:31PM	3.136.39.26	tcp/3000	http	Grafana	HIGH
03:31PM	3.12.117.97	tcp/4443	https	Apache HTTPD, Moodle, Unknown	MEDIUM
03:31PM	3.12.117.97	tcp/800	http	Apache HTTPD, Moodle, Unknown	MEDIUM
03:31PM	18.221.8.100	tcp/8080	http	Apache Tomcat 10.0.21	MEDIUM
03:31PM	3.140.148.113	tcp/8082	http	Apache HTTPD 2.4.25, Drupal CMS, Microsoft Iis	MEDIUM
03:31PM	3.140.148.113	tcp/4443	https	Apache HTTPD 2.4.52, Unknown	MEDIUM
03:31PM	3.133.93.223	tcp/3389	ms-wbt-server	Microsoft Terminal Services	LOW
03:31PM	3.133.93.223	tcp/389	ldap		LOW
03:31PM	3.12.117.97	tcp/22	ssh	OpenBSD OpenSSH 8.2p1 Ubuntu 4ubuntu0.3	LOW
03:31PM	3.128.1.61	tcp/22	ssh	OpenBSD OpenSSH 8.2p1 Ubuntu 4ubuntu0.3	LOW
03:31PM	3.130.245.239	tcp/22	ssh	OpenBSD OpenSSH 8.2p1 Ubuntu 4ubuntu0.3	LOW
03:31PM	3.135.128.226	tcp/22	ssh	OpenBSD OpenSSH 8.2p1 Ubuntu 4ubuntu0.3	LOW
03:31PM	3.136.39.26	tcp/22	ssh	OpenBSD OpenSSH 8.2p1 Ubuntu 4ubuntu0.3	LOW
03:31PM	3.140.148.113	tcp/22	ssh	OpenBSD OpenSSH 8.2p1 Ubuntu 4ubuntu0.3	LOW
03:31PM	13.59.33.147	tcp/22	ssh	OpenBSD OpenSSH 8.2p1 Ubuntu 4ubuntu0.3	LOW
03:31PM	13.59.203.16	tcp/22	ssh	OpenBSD OpenSSH 8.2p1 Ubuntu 4ubuntu0.3	LOW
03:31PM	18.221.8.100	tcp/22	ssh	OpenBSD OpenSSH 8.2p1 Ubuntu 4ubuntu0.3	LOW
03:31PM	20.55.74.97	tcp/22	ssh	OpenBSD OpenSSH 7.4	LOW

First Seen	IP	Port	Iana Service Name	Product	Severity
03:31PM	18.221.8.100	tcp/8443	rtsp		LOW
03:31PM	3.133.93.223	tcp/80	http		LOW
03:31PM	3.133.93.223	tcp/8443	https	VMware Horizon View	LOW
03:31PM	13.59.33.147	tcp/9090	http	Apache HTTPD 2.4.38, Wordpress	LOW
03:31PM	3.133.93.223	tcp/135	msrpc	Microsoft Windows RPC	
03:31PM	3.133.93.223	tcp/636	tcpwrapped		
03:31PM	3.133.93.223	tcp/4001	newoak		
03:31PM	3.133.93.223	tcp/4002	mlchat-proxy		
03:31PM	3.133.93.223	tcp/5985	http	Microsoft HTTPAPI Httpd 2.0	
03:31PM	3.140.148.113	tcp/50000	http	Jenkins Httpd 2.319.3	
03:31PM	20.55.74.97	udp/53	domain		
03:31PM	20.55.74.97	tcp/53	domain		
03:31PM	20.55.74.97	tcp/161	snmp		

3.6. Excluded Assets

No assets were excluded during this pentest.