



ILLUSTRATIVE SAMPLE REPORT

External Penetration Test

Fix Action Report

Sample Environment

Original sample assessment: August 4, 2025

Illustrative findings supplied for demonstration only.

Not a Massive IT client assessment or evidence of client outcomes.

Branding and vendor-specific technical labels have been adapted;
sample findings, dates, and page numbering have been retained.

Massive IT

www.massiveit.com | sales@massiveit.com

(813) 518-5454 | Tampa, Florida | Nationwide service

SAMPLE ONLY - Not a security assessment of your organization.

Table of Contents

CRITICAL Severity

GitLab ExifTool Remote Code Execution Vulnerability	1
Apache Struts 2 Prefixed Parameters OGNL Remote Code Execution Vulnerability	2
Apache Shiro RememberME Cookie Deserialization Remote Code Execution Vulnerability	3
Oracle Weblogic wls-wsat Component XML Deserialization Vulnerability Bypass	4
Oracle Weblogic wls-wsat Component XML Deserialization Vulnerability	5
Apache Struts2 Content Header Remote Code Execution Vulnerability	6
Apache Struts2 S2-048 Remote Code Execution Vulnerability	7
Apache Solr Velocity Remote Code Execution Vulnerability	8
Oracle WebLogic Java Deserialization Vulnerability - Console Component	9
F5 BIG-IP iControl REST Remote Command Execution Vulnerability	10
Atlassian Confluence Namespace OGNL Injection Vulnerability	11
Atlassian Confluence Server - Improper Authorization	12
Weak or Default Credentials - Password Spray	13
JBoss Application Server HTTP Invoker Remote Code Execution Vulnerability	14
Azure Multi-Factor Authentication Disabled	15
Apache mod_proxy Server-Side Request Forgery Vulnerability	16
Apache Log4j2 Remote Code Execution Vulnerability	17
AWS Unrestricted Assume Role Access	18
AWS Instance Metadata Service v1 Exposed	19
AWS Assume Role Access	20
Confluence Hardcoded Credentials Vulnerability	21
Jenkins Arbitrary File Leak Vulnerability	22
Unauthenticated Access to the Jenkins Script Console	23
Unauthenticated Kubernetes API Server Access	24
Weak or Default Credentials - Web Applications	25
Apache Solr Arbitrary File Read Vulnerability	26
Weak or Default Credentials - Microsoft SQL Server	27
Apache Solr DataImportHandler Remote Code Execution Vulnerability	28
Weak or Default Credentials - SSH	29
Unrestricted Sudo Privileges	30
Public Access to Amazon S3 Bucket	31

HIGH Severity

Weak or Default Credentials - MySQL	32
Weak or Default Credentials - Cracked Credentials	33
OpenSSL Heartbleed Vulnerability	34
Apache JServ Protocol (AJP) Vulnerability	35
Grafana Directory Traversal Vulnerability	36
Subdomain Takeover	37
Public Access to Git Repository	38
Web Application Cross Site Scripting Vulnerability	39
Weak or Default Credentials - Telnet	40
Apache Druid Server-Side Request Forgery Vulnerability	41
MEDIUM Severity	
Credential Dumping - /etc/shadow File	42
Unauthenticated Access to Elasticsearch	43
Keycloak request_uri Blind Server-Side Request Forgery Vulnerability	44
Apache Solr Server-Side Request Forgery Vulnerability	45
Jetty Limited Path Traversal Vulnerability - Second Variation	46
Gitlab GraphQL API Unauthenticated User Enumeration	47
Anonymous Access to Printer using PJP or PS	48
Kubernetes Service Account Token Exposure	49
Unauthenticated Access to Apache Solr	50
Unauthenticated Access to Jenkins People Directory	51
Jenkins Self-Signup Enabled	52
Unauthenticated Gitlab User Enumeration	53
Unauthenticated Jenkins Dashboard Exposure	54
Golang pprof Debugging Endpoint Enabled	55
Public Access to Amazon EC2 AMI	56
Public Access to Amazon EBS Snapshot	57
Public Access to Amazon RDS Snapshot	58
Telnet Port Exposed to the Internet	59
Apache Tomcat Example Scripts Exposed	60
LOW Severity	
Anonymous FTP Enabled	61
IIS web.config File Exposure	62
Weak or Default Credentials - SNMP	63
Secure Socket Shell (SSH) Port Exposed to the Internet	64

Database Port Exposed to the Internet	65
File Transfer Protocol (FTP) Port Exposed to the Internet	66
Simple Network Management Protocol (SNMP) Port Exposed to the Internet	67
Web Directory Listing	68
Public-Facing Application Exposed with HTTP Basic Authentication	69
Exposed Kubernetes Version	70
Dangling DNS Record	71
Expired SSL/TLS Certificate	72
Public Self-Signed Certificate	73

GitLab ExifTool Remote Code Execution Vulnerability

CRITICAL 10

CVE-2021-22205

Affected Host

- 184.73.131.205 (ec2-184-73-131-205.compute-1.amazonaws.com)

Mitigations

- Update to the latest Gitlab application version per the vendor advisory. This issue was fixed in the GitLab 13.10.3, 13.9.6, and 13.8.8 release from April 14, 2021.
- Apply the hotpatch per the vendor instructions.

References

- [Gitlab Advisory for CVE-2021-22205](#) 
- [Gitlab Hotpatch Instructions for CVE-2021-22205](#) 
- [Gitlab issue 327121](#) 
- [NVD: CVE-2021-22205](#) 
- [Metasploit: GitLab Unauthenticated Remote ExifTool Command Injection](#) 
- [Nuclei: GitLab CE/EE - Remote Code Execution](#) 

Apache Struts 2 Prefixed Parameters OGNL Remote Code Execution Vulnerability

CRITICAL 9.8

CVE-2013-2251

Affected Host

- 54.91.240.159 (ec2-54-91-240-159.compute-1.amazonaws.com)

Mitigations

- Upgrade to Apache Struts 2.3.15.1 or later per the vendor advisory.

References

- [Apache Advisory and Patches](#) 
- [NVD: CVE-2013-2251](#) 
- [Metasploit: Apache Struts 2 DefaultActionMapper Prefixes OGNL Code Execution](#) 
- [Nuclei: Apache Struts 2 - DefaultActionMapper Prefixes OGNL Code Execution](#) 

Apache Shiro RememberME Cookie Deserialization Remote Code Execution Vulnerability

CRITICAL 9.8

CVE-2016-4437

Affected Host

- 54.91.240.159 (ec2-54-91-240-159.compute-1.amazonaws.com)

Mitigations

- Upgrade to Apache Shiro 1.2.5 or later.

References

- [Vendor Acknowledgement](#) 
- [NVD: CVE-2016-4437](#) 
- [Metasploit: Apache Shiro v1.2.4 Cookie RememberME Deserial RCE](#) 
- [Nuclei: Apache Shiro 1.2.4 Cookie RememberME - Deserial Remote Code Execution Vulnerability](#) 

Oracle Weblogic wls-wsat Component XML Deserialization Vulnerability Bypass

CRITICAL 9.8

CVE-2017-10271

Affected Host

- 54.91.240.159 (ec2-54-91-240-159.compute-1.amazonaws.com)

Mitigations

- Apply the updates provided by the product vendor. The affected versions are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.1.0, and 12.2.1.2.0.

References

- [Oracle Critical Patch Update Advisory - October 2017](#) 
- [NVD: CVE-2017-10271](#) 
- [CVE-2017-10271 Used to Deliver CryptoMiners: An Overview of Techniques Used Post-Exploitation and Pre-Mining](#) 
- [Metasploit: Oracle WebLogic wls-wsat Component Deserialization RCE](#) 
- [Nuclei: Oracle WebLogic Server - Remote Command Execution](#) 

CVE-2017-3506

Affected Host

- 54.91.240.159 (ec2-54-91-240-159.compute-1.amazonaws.com)

Mitigations

- Upgrade Oracle Weblogic by following the directions provided in the Oracle Critical Patch Advisory, or update to the latest version.

References

- [Oracle Critical Patch Update Advisory](#) 
- [Remote OS Command Execution on Oracle Weblogic server via \[CVE-2017-3506\]](#) 
- [8220 Gang Exploiting Oracle WebLogic Flaw to Hijack Servers and Mine Cryptocurrency](#) 
- [NVD: CVE-2017-3506](#) 
- [CISA Adds One Known Exploited Vulnerability to Catalog](#) 
- [Oracle WebLogic Server OS Command Injection Flaw Under Active Attack](#) 
- [Nuclei: Oracle Fusion Middleware Weblogic Server - Remote OS Command Execution](#) 

Apache Struts2 Content Header Remote Code Execution Vulnerability

CRITICAL 9.8

CVE-2017-5638

Affected Host

- 54.91.240.159 (ec2-54-91-240-159.compute-1.amazonaws.com)

Mitigations

- Upgrade to the latest version of Apache Struts. This particular vulnerability is fixed in Struts 2.3.32 and Struts 2.5.10.1. However there are other critical vulnerabilities that warrant updating to the latest version of Struts.

References

- [Apache Struts Security Advisory S2-045](#) 
- [Apache Struts Security Advisory S2-046](#) 
- [NVD: CVE-2017-5638 Detail](#) 
- [Using ModSecurity to Virtually Patch Apache Struts CVE-2017-5638](#) 
- [Metasploit: Apache Struts Jakarta Multipart Parser OGNL Injection](#) 
- [Nuclei: Apache Struts 2 - Remote Command Execution](#) 

Apache Struts2 S2-048 Remote Code Execution Vulnerability

CRITICAL 9.8

CVE-2017-9791

Affected Host

- 54.91.240.159 (ec2-54-91-240-159.compute-1.amazonaws.com)

Mitigations

- Refer to vendor product guidance to update to the latest version.

References

- [S2-048](#) 
- [NVD: CVE-2017-9791 Detail](#) 
- [Metasploit: Apache Struts 2 Struts 1 Plugin Showcase OGNL Code Execution](#) 
- [Nuclei: Apache Struts2 S2-053 - Remote Code Execution](#) 

Apache Solr Velocity Remote Code Execution Vulnerability

CRITICAL 9.8

CVE-2019-17558

Affected Host

- 3.91.156.158 (ec2-3-91-156-158.compute-1.amazonaws.com)

Mitigations

- Upgrade to Apache Solr 8.4 or greater.

References

- [Vendor Advisory](#) 
- [Proof of Concept and Writeup](#) 
- [NVD: CVE-2019-17558](#) 
- [Metasploit: Apache Solr Remote Code Execution via Velocity Template](#) 
- [Nuclei: Apache Solr <=8.3.1 - Remote Code Execution](#) 

CVE-2020-14882

Affected Host

- 54.91.240.159 (ec2-54-91-240-159.compute-1.amazonaws.com)

Mitigations

- Apply all updates and patch to the latest vendor-supported version for both this vulnerability and for the related CVE-2020-14750 vulnerability.

References

- [Oracle Security Advisory for CVE-2020-14882](#) 
- [Oracle Security Advisory for CVE-2020-14750](#) 
- [NVD: CVE-2020-14882](#) 
- [Bug hunting for a quick buck using WebLogic vulnerability \(CVE-2020-14882\)](#) 
- [Metasploit: Oracle WebLogic Server Administration Console Handle RCE](#) 
- [Nuclei: Oracle Weblogic Server - Remote Command Execution](#) 

F5 BIG-IP iControl REST Remote Command Execution Vulnerability

CRITICAL 9.8

CVE-2022-1388

Affected Host

- 4.246.214.129 (f5.pod04.example.com)

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

- Massive IT: F5 iControl REST Endpoint Authentication Bypass Technical Deep Dive 
- [F5 Security Advisory](#) 
- [NVD: CVE-2022-1388](#) 
- [Metasploit: F5 BIG-IP iControl RCE via REST Authentication Bypass](#) 
- [Nuclei: F5 BIG-IP iControl - REST Auth Bypass RCE](#) 

CVE-2022-26134

Affected Host

- 3.91.156.158 (ec2-3-91-156-158.compute-1.amazonaws.com)

Mitigations

- Update to the latest vendor-supported version referenced in the Confluence Security bulletin.
- Follow the mitigation instructions in the Confluence Security Bulletin to manually patch the xwork jar files.

References

- [Confluence Security Bulletin for CVE-2022-26134](#) 
- [Zero-Day Exploitation of Atlassian Confluence](#) 
- [NVD: CVE-2022-26134](#) 
- [CVE-2022-26134 Threat Brief: Atlassian Confluence RCE Vulnerability](#) 
- [Metasploit: Atlassian Confluence Namespace OGNL Injection](#) 
- [Nuclei: Confluence - Remote Code Execution](#) 

Atlassian Confluence Server - Improper Authorization

CRITICAL 9.8

CVE-2023-22518

Affected Host

- 3.91.156.158 (ec2-3-91-156-158.compute-1.amazonaws.com)

Mitigations

- Follow the instructions referenced in the vendor advisory. Atlassian recommends updating to one of the following fixed versions of Confluence Data Center and Server 7.19.16, 8.3.4, 8.4.4, 8.5.3, 8.6.1

References

- [Vendor Advisory](#) 
- [NVD: CVE-2023-22518](#) 
- [Metasploit: Atlassian Confluence Unauth JSON setup-restore Improper Authorization leading to RCE \(CVE-2023-22518\)](#) 
- [Nuclei: Atlassian Confluence Server - Improper Authorization](#) 

PT-2021-0019

Affected Assets

- Microsoft Entra User 79c1f87so8
- Microsoft Entra User kionbobwe2
- Microsoft Entra User 79c1f87so87738
- Microsoft Entra User kionbobwe25867
- Microsoft Entra User 79c1f87so81262
- Microsoft Entra User kionbobwe27885
- Microsoft Entra User kionbobwe2
- Microsoft Entra User kionbobwe2
- Microsoft Entra User kionbobwe2
- Microsoft Entra User kionbobwe2
- Microsoft Entra User kionbobwe2

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** [↗](#)
- **MITRE ATT&CK Technique: T1110: Brute Force** [↗](#)
- **MITRE ATT&CK Technique: T1110.003: Brute Force: Password Spraying** [↗](#)

JBoss Application Server HTTP Invoker Remote Code Execution Vulnerability

CRITICAL 9.8

PT-2021-0047

Affected Host

- 54.91.240.159 (ec2-54-91-240-159.compute-1.amazonaws.com)

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](#) 
- [CISA Analysis Report \(AR18-312A\): JexBoss - JBoss Verify and EXploitation Tool](#) 
- [FoxGlove Security: What Do WebLogic, WebSphere, JBoss, Jenkins, OpenNMS, and Your Application Have in Common?](#) 
- [SAS Guidance: Removing the JMX Console and the EJBInvokerServlet and JMXInvokerServlet applications from the JBoss application server](#) 
- [IBM: JBoss Security Remediation Guidance](#) 
- [MITRE ATT&CK Technique: T1210: Exploitation of Remote Services](#) 

PT-2022-0002

Affected Assets

- Microsoft Entra User 79c1f87so8
- Microsoft Entra User kionbobwe2
- Microsoft Entra User 79c1f87so87738
- Microsoft Entra User 79c1f87so81262
- Microsoft Entra User kionbobwe27885
- Microsoft Entra User kionbobwe25867
- Microsoft Entra User kionbobwe2
- Microsoft Entra User kionbobwe2
- Microsoft Entra User kionbobwe2
- Microsoft Entra User kionbobwe2

Mitigations

- Enable multi-factor authentication for all users to access Azure resources.

References

- [How to Enable Multi-Factor Authentication in Azure](#) 
- [CWE-308: Use of Single-factor Authentication](#) 

Apache mod_proxy Server-Side Request Forgery Vulnerability

CRITICAL 9.6

CVE-2021-40438

Affected Host

- 54.82.213.135 (ec2-54-82-213-135.compute-1.amazonaws.com)

Mitigations

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

References

- [What is SSRF?](#) 
- [Apache 2.4 Vulnerabilities](#) 
- [NVD: CVE-2021-40438](#) 
- [CISA Adds Five Known Exploited Vulnerabilities to Catalog](#) 
- [Nuclei: Apache <= 2.4.48 Mod_Proxy - Server-Side Request Forgery](#) 

Affected Hosts

- 54.82.213.135 (ec2-54-82-213-135.compute-1.amazonaws.com)
- 52.90.237.79 (ec2-52-90-237-79.compute-1.amazonaws.com)
- 52.90.237.79 (ec2-52-90-237-79.compute-1.amazonaws.com)
- 54.145.223.2 (ec2-54-145-223-2.compute-1.amazonaws.com)
- 3.91.156.158 (ec2-3-91-156-158.compute-1.amazonaws.com)
- 184.73.131.205 (ec2-184-73-131-205.compute-1.amazonaws.com)

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 $\geq$ 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 $\geq$ 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 $\geq$ 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

- Massive IT: The Long Tail of Log4Shell Exploitation 
- Massive IT: Understanding Log4Shell: the Apache log4j2 Remote Code Execution Vulnerability 
- **CISA Advisory** 
- **Compilation of Vendor Advisories** 
- **Cheat Sheet Reference Guide** 
- **Apache Log4j2 Release Notes** 
- **NVD: CVE-2021-44228** 
- **Metasploit: Log4Shell HTTP Scanner** 
- **Nuclei: Apache Log4j2 Remote Code Injection** 

AWS Unrestricted Assume Role Access

CRITICAL 9.6

PT-2021-0029

Affected Asset

- AWS Role SamplePentest

Mitigations

- Within the AWS console, find the role, and edit the Trust Relationship to allow a specific AWS Principal instead of a wildcard group.

References

- [AWS - Creating Roles for External IDs](#) 
- [MITRE ATT&CK Technique: T1548.005: Abuse Elevation Control Mechanism: Temporary Elevated Cloud Access](#) 

AWS Instance Metadata Service v1 Exposed

CRITICAL 9.6

PT-2021-0040

Affected Hosts

- 54.82.213.135 (ec2-54-82-213-135.compute-1.amazonaws.com)
- 18.224.215.223 (ec2-18-224-215-223.us-east-2.compute.amazonaws.com)

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](#)
- [MITRE ATT&CK Technique: T1552.005: Unsecured Credentials: Cloud Instance Metadata API](#)

PT-2022-0074

Affected Assets

- AWS Role list-role
- AWS Role read-role
- AWS Role write-role
- AWS Role assuming-role
- AWS Role hard-to-guess-305199
- AWS Role audit

Mitigations

- Within the AWS console, find the role, and review the Trust Relationship to make sure only the users and groups that need that role can assume it.

References

- [Security Best Practices for AWS IAM](#) 
- [MITRE ATT&CK Technique: T1548.005: Abuse Elevation Control Mechanism: Temporary Elevated Cloud Access](#) 

Confluence Hardcoded Credentials Vulnerability

CRITICAL 9.5

CVE-2022-26138

Affected Host

- 3.91.156.158 (ec2-3-91-156-158.compute-1.amazonaws.com)

Mitigations

- Update to a non-vulnerable version of Questions for Confluence.
- Disable or delete the disabledsystemuser account.

References

- [Questions For Confluence Security Advisory 2022-07-20](#) 
- [NVD: CVE-2022-26138](#) 
- [Latest Critical Atlassian Confluence Vulnerability Under Active Exploitation](#) 
- [Nuclei: Atlassian Questions For Confluence - Hardcoded Credentials](#) 

Jenkins Arbitrary File Leak Vulnerability

CRITICAL 9.5

CVE-2024-23897

Affected Hosts

- 34.204.0.143 (ec2-34-204-0-143.compute-1.amazonaws.com)
- 18.208.189.246 (ec2-18-208-189-246.compute-1.amazonaws.com)

Mitigations

- Upgrade to at least Jenkins 2.442 or Jenkins LTS 2.426.3
- Apply the mitigation from the Jenkins Patch Workaround reference. The workaround disables the Jenkins CLI.

References

- Massive IT: Assessing the Impact of the Jenkins Arbitrary File Leak Vulnerability 
- [Jenkins Advisory](#) 
- [Jenkins Patch Workaround](#) 
- [SonarSource Researcher Writeup](#) 
- [NVD: CVE-2024-23897](#) 
- [CISA Adds One Known Exploited Vulnerability to Catalog](#) 
- [Metasploit: Jenkins cli Ampersand Replacement Arbitrary File Read](#) 
- [Nuclei: Jenkins < 2.441 - Arbitrary File Read](#) 

Unauthenticated Access to the Jenkins Script Console

CRITICAL 9.5

PT-2020-0021

Affected Hosts

- 18.208.189.246 (ec2-18-208-189-246.compute-1.amazonaws.com)
- 34.204.0.143 (ec2-34-204-0-143.compute-1.amazonaws.com)

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](#) 
- [Jenkins - Script-Console Java Execution \(Metasploit\)](#) 
- [MITRE ATT&CK Technique: T1059: Command and Scripting Interpreter](#) 

PT-2021-0006

Affected Host

- 3.85.52.200 (ec2-3-85-52-200.compute-1.amazonaws.com)

Mitigations

- Review the RBAC permissions to Kubernetes API server for the anonymous and default service account.
- Explicitly specify a Service Account for all of your workloads (serviceAccountName in Pod.Spec), and manage their permissions according to the least privilege principal.
- Consider opting out automatic mounting of SA token using automountServiceAccountToken: false on ServiceAccount resource or Pod.spec.
- Do not enable kube-api's --insecure-port flag in production and ensure the kube-api is exposed only on an HTTPS port.

References

- [Configure Service Accounts for Pods](#) 
- [Using RBAC Authorization](#) 
- [CIS Benchmarks: Securing Kubernetes](#) 
- [MITRE ATT&CK Technique: T1609: Container Administration Command](#) 
- [MITRE ATT&CK Technique: T1613: Container and Resource Discovery](#) 

PT-2021-0021

Affected Hosts

- 3.91.156.158 (ec2-3-91-156-158.compute-1.amazonaws.com)
- 54.91.240.159 (ec2-54-91-240-159.compute-1.amazonaws.com)
- 3.91.156.158 (ec2-3-91-156-158.compute-1.amazonaws.com)
- 18.208.189.246 (ec2-18-208-189-246.compute-1.amazonaws.com)
- 54.91.240.159 (ec2-54-91-240-159.compute-1.amazonaws.com)
- 3.91.156.158 (ec2-3-91-156-158.compute-1.amazonaws.com)

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** [↗](#)
- **MITRE ATT&CK Technique: T1110: Brute Force** [↗](#)
- **MITRE ATT&CK Technique: T1078.001: Valid Accounts: Default Accounts** [↗](#)

Apache Solr Arbitrary File Read Vulnerability

CRITICAL 9.4

PT-2023-0023

Affected Hosts

- 3.91.156.158 (ec2-3-91-156-158.compute-1.amazonaws.com)
- 184.73.131.205 (ec2-184-73-131-205.compute-1.amazonaws.com)

Mitigations

- Enable authentication and authorization using the reference plugin.
- Configure an allow list of device IP addresses that can communicate with the Solr server.

References

- [Configuring Authentication, Authorization and Audit Logging](#) 
- [Apache Solr Security Advisory](#) 
- [Apache Solr Arbitrary File Read and SSRF Vulnerability Threat Alert](#) 
- [Apache Solr Security News](#) 
- [NVD: CVE-2021-27905 Detail](#) 

PT-2021-0016

Affected Host

- 54.166.18.219 (ec2-54-166-18-219.compute-1.amazonaws.com)

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** [↗](#)
- **MITRE ATT&CK Technique: T1110: Brute Force** [↗](#)
- **MITRE ATT&CK Technique: T1078.001: Valid Accounts: Default Accounts** [↗](#)

CVE-2019-0193

Affected Host

- 3.91.156.158 (ec2-3-91-156-158.compute-1.amazonaws.com)

Mitigations

- Upgrade to 8.2.0 or later, which is secure by default.
- Edit solrconfig.xml to configure all DataImportHandler usages with an "invariants" section listing the "dataConfig" parameter set to an empty string. Example: `<requestHandler name="/dataimport" class="org.apache.solr.handler.dataimport.DataImportHandler"> <lst name="invariants"> <str name="dataConfig"></str> </lst> </requestHandler>`
- Ensure your network settings are configured so that only trusted traffic communicates with Solr, especially to the DIH request handler. This is a best practice to all of Solr.

References

- [Vendor Advisory](#) 
- [NVD: CVE-2019-0193](#) 
- [Nuclei: Apache Solr DataImportHandler <8.2.0 - Remote Code Execution](#) 

PT-2021-0014

Affected Hosts

- 54.145.223.2 (ec2-54-145-223-2.compute-1.amazonaws.com)
- 3.91.156.158 (ec2-3-91-156-158.compute-1.amazonaws.com)

Table of Contents

- **Option 1: Implement a Strong Password Policy**
- **Option 2: Implement a Configuration Management Policy**

Option 1: Implement a Strong Password Policy

Change the credential's password and ensure a strong password policy is in place and users are properly trained on best practices. The National Institute of Standards and Technology (NIST) commonly releases guidance on password best practices which include:

- A minimum length of 8 characters
- Blacklisting passwords that contain dictionary words, repetitive or sequential characters, and the company name
- Implement Multi-Factor Authentication when available

NOTE: See full NIST publication here [NIST 800-63-3](#)

Option 2: Implement a Configuration Management Process

Often, systems and applications will be installed without the default credentials being changed. Identify a configuration management process that ensures default credentials are changed before systems are deployed in a production environment.

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** [↗](#)
- **MITRE ATT&CK Technique: T1110: Brute Force** [↗](#)
- **MITRE ATT&CK Technique: T1078.001: Valid Accounts: Default Accounts** [↗](#)

Unrestricted Sudo Privileges

CRITICAL 9.2

PT-2021-0039

Affected Host

- 54.145.223.2 (ec2-54-145-223-2.compute-1.amazonaws.com)

Mitigations

- Determine if the user requires arbitrary root-level privileges. If it makes sense, modify the sudo configuration so that the user can only run a restricted set of commands as root with sudo.

References

- [How to Edit the Sudoers File](#) 
- [MITRE ATT&CK Technique: T1548.003: Abuse Elevation Control Mechanism: Sudo and Sudo Caching](#) 

Public Access to Amazon S3 Bucket

CRITICAL 9

PT-2021-0001

Affected Assets

- S3 Bucket stooge-sultry-substance
- S3 Bucket primer-multitask-preplan

Mitigations

- Verify that the bucket is in fact owned by your company. The bucket that was found has a name similar to one of your company's subdomains.
- Review the data contained in the bucket, and remove any data that should not be exposed.
- Review bucket and object permissions for anonymous and any authenticated (cross-account) AWS users. Apply least-privilege permissions as appropriate.

References

- [Security Best Practices for AWS S3](#) 
- [How can I secure the files in my Amazon S3 bucket?](#) 
- [MITRE ATT&CK Technique: T1530: Data from Cloud Storage](#) 

PT-2021-0017

Affected Host

- 54.166.18.219 (ec2-54-166-18-219.compute-1.amazonaws.com)

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](#) 
- [MITRE ATT&CK Technique: T1110: Brute Force](#) 
- [MITRE ATT&CK Technique: T1078.001: Valid Accounts: Default Accounts](#) 

PT-2021-0020

Affected Assets

- Cleartext Password for user
- Cleartext Password for root
- Cleartext Password for root

Table of Contents

- **Option 1: Implement a Strong Password Policy**
- **Option 2: Implement a Configuration Management Process**

Option 1: Implement a Strong Password Policy

Change the credential's password and ensure a strong password policy is in place and users are properly trained on best practices. The National Institute of Standards and Technology (NIST) commonly releases guidance on password best practices which include:

- A minimum length of 8 characters
- Blacklisting passwords that contain dictionary words, repetitive or sequential characters, and the company name
- Implement Multi-Factor Authentication when available

NOTE: See full NIST publication here [NIST 800-63-3](#)

Option 2: Implement a Configuration Management Process

Often, systems and applications will be installed without the default credentials being changed. Identify a configuration management process that ensures default credentials are changed before systems are deployed in a production environment.

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** [↗](#)
- **MITRE ATT&CK Technique: T1110: Brute Force** [↗](#)
- **MITRE ATT&CK Technique: T1110.002: Brute Force: Password Cracking** [↗](#)

OpenSSL Heartbleed Vulnerability

HIGH 7.5

CVE-2014-0160

Affected Host

- 54.166.18.219 (ec2-54-166-18-219.compute-1.amazonaws.com)

Mitigations

- The vulnerability is patched in OpenSSL version 1.0.1g and later. Refer to your vendor's documentation to upgrade to the latest version.

References

- [Heartbleed](#) 
- [FOX-IT Blog Writeup](#) 
- [NVD: CVE-2014-0160](#) 
- [Oracle Security Alert for CVE-2014-0160](#) 
- [Attackers Exploit the Heartbleed OpenSSL Vulnerability to Circumvent Multi-factor Authentication on VPNs](#) 
- [OpenSSL Heartbleed Vulnerability CVE-2014-0160](#) 
- [OpenSSL Heartbleed vulnerability CVE-2014-0160 - Cisco products and mitigations - Cisco Blogs](#) 
- [Metasploit: OpenSSL Heartbeat \(Heartbleed\) Information Leak](#) 

Apache JServ Protocol (AJP) Vulnerability

HIGH 7.5

CVE-2020-1938

Affected Host

- 18.208.189.246 (ec2-18-208-189-246.compute-1.amazonaws.com)

Mitigations

- Update to the latest version of Apache Tomcat. Apache Tomcat has released versions 9.0.31, 8.5.51, and 7.0.100 to fix this vulnerability.
- Red Hat recommends disabling the Apache JServ Protocol (AJP) connector in Tomcat if not used, or binding it to localhost port, since most of AJP's use is in cluster environments. The AJP connector port should never be exposed on the internet without strict access-control lists. The AJP connector is enabled by default on all Tomcat servers.
- If the AJP service does not need to be publicly accessible, ensure that access is filtered.

References

- [NVD: CVE-2020-1938](#) 
- [Metasploit: Apache Tomcat AJP File Read](#) 
- [Nuclei: Ghostcat - Apache Tomcat - AJP File Read/Inclusion Vulnerability](#) 

Grafana Directory Traversal Vulnerability

HIGH 7.5

CVE-2021-43798

Affected Host

- 54.91.240.159 (ec2-54-91-240-159.compute-1.amazonaws.com)

Mitigations

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

References

- [An update on Oday CVE-2021-43798: Grafana directory traversal](#) 
- [NVD: CVE-2021-43798](#) 
- [Assessing Potential Exploitation of Grafana's CVE-2021-43798 for Initial Access](#) 
- [Metasploit: Grafana Plugin Path Traversal](#) 
- [Nuclei: Grafana v8.x - Arbitrary File Read](#) 

PT-2021-0002

Affected Host

- 52.219.93.248

Table of Contents

- [Option 1: Remove Dangling CNAME](#)
- [Option 2: Update CNAME](#)

Option 1: Remove Dangling CNAME

1. If the subdomain is no longer in use, then from your DNS zone, remove the subdomain's DNS record.
 2. Review application code and configuration for references to subdomains no longer in use and remove those references.
-

Option 2: Update the CNAME

1. If the subdomain is still in use, update the subdomain's DNS record so that its CNAME(s) point to valid resources.
-

References

- [Subdomain Takeovers: Thoughts on Risk](#)
- [Prevent Dangling DNS Entries and Avoid Subdomain Takeover](#)

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](#) 
- [Prevent Dangling DNS Entries and Avoid Subdomain Takeover](#) 
- [MITRE ATT&CK Technique: T1584.001: Compromise Infrastructure: Domains](#) 

Public Access to Git Repository

HIGH 7.5

PT-2021-0031

Affected Assets

- Git Repo fakegit
- Git Repo Test_truffle
- Git Repo secret_test
- Git Repo fakegit2

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](#) 
- [Security Best Practices for Git Users](#) 
- [10 GitHub Security Best Practices](#) 
- [Removing sensitive data from a repository](#) 
- [MITRE ATT&CK Technique: T1213.003: Data from Information Repositories: Code Repositories](#) 

Web Application Cross Site Scripting Vulnerability

HIGH 7.5

PT-2022-0001

Affected Hosts

- 34.200.173.81 (ec2-34-200-173-81.compute-1.amazonaws.com)
- 34.200.173.81 (ec2-34-200-173-81.compute-1.amazonaws.com)

Mitigations

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

References

- [Cross Site Scripting \(XSS\)](#) 
- [MITRE ATT&CK Technique: T1203: Exploitation for Client Execution](#) 

Weak or Default Credentials - Telnet

HIGH 7

PT-2021-0013

Affected Host

- 54.166.18.219 (ec2-54-166-18-219.compute-1.amazonaws.com)

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** [↗](#)
- **MITRE ATT&CK Technique: T1110: Brute Force** [↗](#)
- **MITRE ATT&CK Technique: T1078.001: Valid Accounts: Default Accounts** [↗](#)

Apache Druid Server-Side Request Forgery Vulnerability

HIGH 7

PT-2021-0041

Affected Hosts

- 52.90.237.79 (ec2-52-90-237-79.compute-1.amazonaws.com)
- 52.90.237.79 (ec2-52-90-237-79.compute-1.amazonaws.com)

Mitigations

- Implement authentication on the server.

References

- [Security Best Practices for Apache Druid](#) 

Credential Dumping - /etc/shadow File

MEDIUM 6.7

PT-2021-0045

Affected Hosts

- 54.145.223.2 (ec2-54-145-223-2.compute-1.amazonaws.com)
- 4.246.214.129 (f5.pod04.example.com)

Mitigations

- Set up and configure a monitoring tool, such as auditd, to monitor and audit access to the /etc/shadow file and other files containing sensitive data.
- Ensure all privileged accounts have complex unique passwords to prevent attackers from being able to crack their password hashes and pivot with them to other systems.
- Follow best practices to restrict account permissions and access to privileged accounts.

References

- [Red Hat: How to monitor permission, ownership or any other change to a particular directory or file](#) 
- [MITRE ATT&CK Technique: OS Credential Dumping: /etc/passwd and /etc/shadow](#) 

Unauthenticated Access to Elasticsearch

MEDIUM 6

PT-2021-0036

Affected Host

- 54.145.223.2 (ec2-54-145-223-2.compute-1.amazonaws.com)

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](#) 
- [MITRE ATT&CK Technique: T1210: Exploitation of Remote Services](#) 

Keycloak request_uri Blind Server-Side Request Forgery Vulnerability

MEDIUM 5.3

CVE-2020-10770

Affected Host

- 54.145.223.2 (ec2-54-145-223-2.compute-1.amazonaws.com)

Mitigations

- This vulnerability affects Keycloak versions before 13.0.0. Upgrade the product to the latest version.

References

- [Keycloak 12.0.1 Server-Side Request Forgery #8776; Packet Storm](#) 
- [CVE-2020-10770 keycloak: Default Client configuration is vulnerable to SSRF using the "request_uri" parameter](#) 
- [NVD: CVE-2020-10770](#) 
- [Nuclei: Keycloak <= 12.0.1 - request_uri Blind Server-Side Request Forgery \(SSRF\)](#) 

Apache Solr Server-Side Request Forgery Vulnerability

MEDIUM 5.3

CVE-2021-27905

Affected Hosts

- 3.91.156.158 (ec2-3-91-156-158.compute-1.amazonaws.com)
- 184.73.131.205 (ec2-184-73-131-205.compute-1.amazonaws.com)

Mitigations

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

References

- [What is SSRF?](#) 
- [Apache Solr Security News](#) 
- [NVD: CVE-2021-27905](#) 
- [Nuclei: Apache Solr <=8.8.1 - Server-Side Request Forgery](#) 

Jetty Limited Path Traversal Vulnerability - Second Variation

MEDIUM 5.3

CVE-2021-34429

Affected Host

- 34.204.0.143 (ec2-34-204-0-143.compute-1.amazonaws.com)

Mitigations

- Update to Jetty version 9.4.43, 10.0.6, 11.0.6 or later.

References

- [Encoded URIs can access WEB-INF](#) 
- [NVD: CVE-2021-34429](#) 
- [Metasploit: Jetty WEB-INF File Disclosure](#) 
- [Nuclei: Eclipse Jetty - Information Disclosure](#) 

Gitlab GraphQL API Unauthenticated User Enumeration

MEDIUM 5.3

CVE-2021-4191

Affected Host

- 18.215.183.13 (ec2-18-215-183-13.compute-1.amazonaws.com)

Mitigations

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

References

- [Gitlab Critical Security Release: 14.8.2, 14.7.4, and 14.6.5](#) ↗
- [NVD: CVE-2021-4191](#) ↗
- [Metasploit: GitLab GraphQL API User Enumeration](#) ↗
- [Nuclei: GitLab GraphQL API User Enumeration](#) ↗

Anonymous Access to Printer using PjL or PS

MEDIUM 5

PT-2020-0003

Affected Host

- 54.166.18.219 (ec2-54-166-18-219.compute-1.amazonaws.com)

Mitigations

- Disable printing over port 9100, or disable anonymous access by configuring passwords for PjL and file system access.

References

- [CWE-200: Exposure of Sensitive Information to an Unauthorized Actor](#) 
- [Printer Exploitation Toolkit](#) 

Kubernetes Service Account Token Exposure

MEDIUM 5

PT-2021-0007

Affected Host

- 3.85.52.200 (ec2-3-85-52-200.compute-1.amazonaws.com)

Mitigations

- Explicitly specify a service account for all of your workloads (serviceAccountName in Pod.Spec), and manage their permissions according to the least privilege principle.
- Consider opting out of automatic mounting of SA token using automountServiceAccountToken: false on ServiceAccount resource or Pod.spec.
- Review the RBAC permissions to Kubernetes API server for the anonymous and default service account.

References

- [Configure Service Accounts for Pods](#) 
- [Using RBAC Authorization](#) 
- [CIS Benchmarks: Securing Kubernetes](#) 
- [MITRE ATT&CK Technique: T1528: Steal Application Access Token](#) 

Unauthenticated Access to Apache Solr

MEDIUM 5

PT-2022-0028

Affected Hosts

- 3.91.156.158 (ec2-3-91-156-158.compute-1.amazonaws.com)
- 184.73.131.205 (ec2-184-73-131-205.compute-1.amazonaws.com)

Mitigations

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

References

- [Basic Authentication Plugin](#) 
- [Securing Solr With Basic Authentication](#) 
- [MITRE ATT&CK Technique: T1213: Data from Information Repositories](#) 

Unauthenticated Access to Jenkins People Directory

MEDIUM 5

PT-2022-0033

Affected Hosts

- 18.208.189.246 (ec2-18-208-189-246.compute-1.amazonaws.com)
- 34.204.0.143 (ec2-34-204-0-143.compute-1.amazonaws.com)

Mitigations

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

References

- [Managing Security](#) 
- [Access granted with Overall/Read](#) 
- [MITRE ATT&CK Technique: T1087: Account Discovery](#) 

Jenkins Self-Signup Enabled

MEDIUM 5

PT-2022-0071

Affected Hosts

- 34.204.0.143 (ec2-34-204-0-143.compute-1.amazonaws.com)
- 18.208.189.246 (ec2-18-208-189-246.compute-1.amazonaws.com)

Mitigations

- Disable self signup by going to Manage Jenkins -> Configure Global Security -> Security Realm -> ensure "Allow users to sign up" is unchecked.
- Ensure that users who are allowed to self-register have no permissions within the Jenkins application by default.

References

- [Researchers found misconfigured Jenkins servers leaking sensitive data](#) 

Unauthenticated Gitlab User Enumeration

MEDIUM 5

PT-2022-0078

Affected Host

- 184.73.131.205 (ec2-184-73-131-205.compute-1.amazonaws.com)

Mitigations

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

References

- [Project and group visibility](#) 
- [MITRE ATT&CK Technique: T1087: Account Discovery](#) 

Unauthenticated Jenkins Dashboard Exposure

MEDIUM 5

PT-2023-0026

Affected Hosts

- 18.208.189.246 (ec2-18-208-189-246.compute-1.amazonaws.com)
- 34.204.0.143 (ec2-34-204-0-143.compute-1.amazonaws.com)

Mitigations

- Enable security through authentication using the guide provided by Jenkins.

References

- [Securing Jenkins](#) 

Golang pprof Debugging Endpoint Enabled

MEDIUM 4.5

PT-2022-0039

Affected Host

- 3.85.52.200 (ec2-3-85-52-200.compute-1.amazonaws.com)

Mitigations

- Ensure that net/http/pprof endpoints are not exposed to the internet.

References

- [Your pprof is showing](#) 
- [GO Documentation](#) 

Public Access to Amazon EC2 AMI

MEDIUM 4.5

PT-2022-0088

Affected Asset

- AWS EC2 Resource arn:aws:ec2:us-east-2:691429674719:image/ami-03fbf714e4910ff68

Mitigations

- Remove public access to the Amazon EC2 AMI if it does not need to be public.
- If it needs to remain publicly accessible, remove all sensitive information from the AMI including browser history and stored passwords.

References

- [AWS Best Practice - Share EC2 AMI with Only Specific AWS Accounts](#) 
- [MITRE ATT&CK Technique: T1526: Cloud Service Discovery](#) 

Public Access to Amazon EBS Snapshot

MEDIUM 4.5

PT-2022-0089

Affected Asset

- AWS EC2 Resource arn:aws:ec2:us-east-2:691429674719:snapshot/snap-06a19b9d04f902946

Mitigations

- Remove public access to the Amazon EBS Snapshot if it does not need to be public.
- If it needs to remain publicly accessible, remove all sensitive information from the snapshot including browser history and stored passwords.

References

- [AWS Best Practice - Prevent EBS Public Snapshots](#) 
- [MITRE ATT&CK Technique: 1530: Data from Cloud Storage](#) 

Public Access to Amazon RDS Snapshot

MEDIUM 4.5

PT-2022-0090

Affected Asset

- AWS RDS Resource arn:aws:rds:us-east-1:691429674719:snapshot:database-take-1-final-snapshot

Mitigations

- Remove public access to the Amazon RDS Snapshot if it does not need to be public.
- If it needs to remain publicly accessible, remove all sensitive information from the RDS database snapshot.

References

- [AWS Best Practice - Prevent RDS Public Snapshots](#) 
- [MITRE ATT&CK Technique: T1530: Data from Cloud Storage](#) 

Telnet Port Exposed to the Internet

MEDIUM 4

PT-2022-0007

Affected Host

- 54.166.18.219 (ec2-54-166-18-219.compute-1.amazonaws.com)

Mitigations

- Disable the telnet service wherever possible and use SSH in its place.
- 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

- [Hacker leaks passwords for more than 500,000 servers, routers, and IoT devices](#) 
- [Wikipedia: Telnet](#) 
- [MITRE ATT&CK Technique: T1133: External Remote Services](#) 

Apache Tomcat Example Scripts Exposed

MEDIUM 4

PT-2022-0047

Affected Host

- 18.208.189.246 (ec2-18-208-189-246.compute-1.amazonaws.com)

Mitigations

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

References

- [Apache Tomcat vulnerabilities](#) 

Anonymous FTP Enabled

LOW 3.9

PT-2020-0005

Affected Host

- 184.73.131.205 (ec2-184-73-131-205.compute-1.amazonaws.com)

Mitigations

- Disable anonymous login or disable the FTP service if not needed.

References

- [CWE-284: Improper Access Control](#) 
- [MITRE ATT&CK Technique: T1021: Remote Services](#) 

IIS web.config File Exposure

LOW 3.5

PT-2022-0049

Affected Hosts

- 34.204.0.143 (ec2-34-204-0-143.compute-1.amazonaws.com)
- 54.91.240.159 (ec2-54-91-240-159.compute-1.amazonaws.com)

Mitigations

- Restrict access to these files.

References

- [Web.config file exposed vulnerability](#) 

PT-2021-0015

Affected Hosts

- 184.73.131.205 (ec2-184-73-131-205.compute-1.amazonaws.com)
- 184.73.131.205 (ec2-184-73-131-205.compute-1.amazonaws.com)

Table of Contents

- **Option 1: Disable the SNMP Service**
- **Option 2: Update the Community String to a Strong Password**

Option 1: Disable the SNMP Service

If the service is not in use, the best mitigation is to disable it. With a wide variety of devices possible running the SNMP service, instructions for updating SNMP settings is not a one-size fits all solution. Typically instructions can be found on the vendor website. If none are available, SNMP settings can often be configured in the webpage of that device in the network settings.

Option 2: Update the Community String to a Strong Password

With a wide variety of devices possible running the SNMP service, updating the SNMP community string is not a one-size fits all solution. Typically instructions for updating the SNMP community string can be found on the vendor website. If none are available, SNMP community string settings can often be configured in the webpage of that device in the network settings.

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** [↗](#)
- **MITRE ATT&CK Technique: T1110: Brute Force** [↗](#)
- **MITRE ATT&CK Technique: T1078.001: Valid Accounts: Default Accounts** [↗](#)

PT-2022-0005

Affected Hosts

- 3.89.147.161 (ec2-3-89-147-161.compute-1.amazonaws.com)
- 52.90.237.79 (ec2-52-90-237-79.compute-1.amazonaws.com)
- 54.145.223.2 (ec2-54-145-223-2.compute-1.amazonaws.com)
- 18.208.189.246 (ec2-18-208-189-246.compute-1.amazonaws.com)
- 18.215.183.13 (ec2-18-215-183-13.compute-1.amazonaws.com)
- 54.145.223.2 (ec2-54-145-223-2.compute-1.amazonaws.com)
- 184.73.131.205 (ec2-184-73-131-205.compute-1.amazonaws.com)
- 34.200.173.81 (ec2-34-200-173-81.compute-1.amazonaws.com)
- 54.91.240.159 (ec2-54-91-240-159.compute-1.amazonaws.com)
- 3.91.156.158 (ec2-3-91-156-158.compute-1.amazonaws.com)
- 34.204.0.143 (ec2-34-204-0-143.compute-1.amazonaws.com)
- 54.82.213.135 (ec2-54-82-213-135.compute-1.amazonaws.com)
- 3.91.156.158 (ec2-3-91-156-158.compute-1.amazonaws.com)
- 4.246.214.129 (f5.pod04.example.com)
- 54.166.18.219 (ec2-54-166-18-219.compute-1.amazonaws.com)
- 3.85.52.200 (ec2-3-85-52-200.compute-1.amazonaws.com)
- 3.87.45.243 (ec2-3-87-45-243.compute-1.amazonaws.com)

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.
- Disable root users from being able to log in over SSH.
- Limit access to remote management services on hosts to specific management hosts to reduce overall attack surface.

References

- [Eight ways to protect SSH access on your system](#) 
- [AWS EC2 SSH Best Practices](#) 
- [MITRE ATT&CK Technique: T1133: External Remote Services](#) 

Database Port Exposed to the Internet

LOW 3

PT-2022-0006

Affected Hosts

- 54.166.18.219 (ec2-54-166-18-219.compute-1.amazonaws.com)
- 54.166.18.219 (ec2-54-166-18-219.compute-1.amazonaws.com)

Mitigations

- Ensure services exposing data are available to internal networks only.
- Ensure complex passwords are in use for all service accounts.
- Limit access to database services to hosts with a specific need to reduce overall attack surface.

References

- [Database Security](#) 
- [MITRE ATT&CK Technique: T1133: External Remote Services](#) 

File Transfer Protocol (FTP) Port Exposed to the Internet

LOW 3

PT-2022-0008

Affected Host

- 184.73.131.205 (ec2-184-73-131-205.compute-1.amazonaws.com)

Mitigations

- Ensure services exposing data are available to internal networks only.
- Ensure complex passwords are in use for all service accounts.
- Limit access to FTP services to hosts with a specific need to reduce overall attack surface.

References

- [What is FTP?](#) 
- [What is FTP and how does an FTP work?](#) 
- [MITRE ATT&CK Technique: T1133: External Remote Services](#) 

Simple Network Management Protocol (SNMP) Port Exposed to the Internet

LOW 3

PT-2022-0009

Affected Host

- 184.73.131.205 (ec2-184-73-131-205.compute-1.amazonaws.com)

Mitigations

- Disable the SNMP service when not in use.
- Only expose SNMP services to internal networks.
- Limit access to SNMP services to hosts with a specific need to reduce overall attack surface.

References

- [Internet Accessible SNMP Server](#) 
- [MITRE ATT&CK Technique: T1133: External Remote Services](#) 

Web Directory Listing

LOW 3

PT-2022-0069

Affected Hosts

- 18.208.189.246 (ec2-18-208-189-246.compute-1.amazonaws.com)
- 18.208.189.246 (ec2-18-208-189-246.compute-1.amazonaws.com)
- 34.204.0.143 (ec2-34-204-0-143.compute-1.amazonaws.com)

Mitigations

- Disable directory listing on the web server.

References

- [CWE-552](#) 
- [Disable directory listing in Apache](#) 
- [Disable directory listing in nginx](#) 

PT-2022-0075

Affected Hosts

- 18.208.189.246 (ec2-18-208-189-246.compute-1.amazonaws.com)
- 54.166.18.219 (ec2-54-166-18-219.compute-1.amazonaws.com)

Mitigations

- Configure your network to prevent public access to this application.
- Replace basic authentication with a more secure authentication mechanism such as token-based authentication and multi-factor authentication (MFA).

References

- [CWE-287: Improper Authentication](#) 

Exposed Kubernetes Version

LOW 2

PT-2022-0082

Affected Host

- 3.85.52.200 (ec2-3-85-52-200.compute-1.amazonaws.com)

Mitigations

- Modify the KubeletConfiguration file by setting the enableDebuggingHandlers bool to false.

References

- [Kubelet Configuration](#) 
- [MITRE ATT&CK Technique: T1518: Software Discovery](#) 

Dangling DNS Record

LOW 0.1

PT-2021-0024

Affected Assets

- sip.example.com
- doodle.goat.example.com

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](#) 
- [Prevent Dangling DNS Entries and Avoid Subdomain Takeover](#) 
- [MITRE ATT&CK Technique: T1584.001: Compromise Infrastructure: Domains](#) 

Expired SSL/TLS Certificate

LOW 0.1

PT-2021-0025

Affected Hosts

- 3.85.52.200 (ec2-3-85-52-200.compute-1.amazonaws.com)
- 3.87.45.243 (ec2-3-87-45-243.compute-1.amazonaws.com)
- 54.166.18.219 (ec2-54-166-18-219.compute-1.amazonaws.com)
- 34.204.0.143 (ec2-34-204-0-143.compute-1.amazonaws.com)

Mitigations

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

References

- [Let's Encrypt](#) 
- [Public Key Certificate](#) 
- [HTTP Strict Transport Security](#) 

PT-2021-0026

Affected Hosts

- 4.246.214.129 (f5.pod04.example.com)
- 3.87.45.243 (ec2-3-87-45-243.compute-1.amazonaws.com)
- 54.145.223.2 (ec2-54-145-223-2.compute-1.amazonaws.com)
- 34.200.173.81 (ec2-34-200-173-81.compute-1.amazonaws.com)
- 54.166.18.219 (ec2-54-166-18-219.compute-1.amazonaws.com)
- 34.204.0.143 (ec2-34-204-0-143.compute-1.amazonaws.com)

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](#) 
- [Self-Signed Certificate](#) 
- [HTTP Strict Transport Security](#) 