Threat Prioritization List

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.

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.

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.

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. **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)

REFERENCES

1. Siber Güvenlik Bülteni - Ocak 2024. (January 31, 2024). ISR - Information Security Research. https://www.linkedin.com/pulse/siber-güvenlik-bülteni-ocak-2024-jdf2f/
2. Kaya, A. (February 11, 2024). Ivanti CVE-2024-21887, CVE-2023-46805, CVE-2024-21893 ve CVE-2024-21888 Güvenlik Açıkları. Cyber Shield Community. https://cybershieldcommunity.com/ivanti-cve-2024-21887-cve-2023-46805-cve-2024-21893-ve-cve-2024-21888-guvenlik-aciklari/
3. 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. https://www.mandiant.com/resources/blog/suspected-apt-targets-ivanti-zero-day
4. 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. https://arcticwolf.com/resources/blog/cve-2024-21887-cve-2023-46805/
5. Timalsina, R. (February 5, 2024). Mitigate Ivanti Vulnerabilities: CISA Issues Emergency Directive. TuxCare. https://tuxcare.com/blog/mitigate-ivanti-vulnerabilities-cisa-issues-emergency-directive/
6. 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. https://www.volexity.com/blog/2024/01/10/active-exploitation-of-two-zero-day-vulnerabilities-in-ivanti-connect-secure-vpn/
7. Shah, S., & Pindur, D. (January 18, 2024). High Signal Detection and Exploitation of Ivanti's Pulse Connect Secure Auth Bypass & RCE. Assetnote. https://www.assetnote.io/resources/research/high-signal-detection-and-exploitation-of-ivantis-pulse-connect-secure-auth-bypass-rce
8. Eviden Threat Intelligence Team. (January 23, 2024). Analysis of Ivanti 0-days, CVE-2023-46805 & CVE-2024-21887. Atos. https://atos.net/en/lp/securitydive/analysis-of-ivanti-0-days-cve-2023-46805-and-cve-2024-21887
9. Gatlan, S. (January 10, 2024). Ivanti warns of Connect Secure zero-days exploited in attacks. Bleeping Computer. https://www.bleepingcomputer.com/news/security/ivanti-warns-of-connect-secure-zero-days-exploited-in-attacks/
10. iblue.team. Ivanti Connect Secure Auth Bypass and Remote Code Authentication CVE-2024-21887. https://www.iblue.team/incident-response-1/ivanti-connect-secure-auth-bypass-and-remote-code-authentication-cve-2024-21887
11. Beaumont, K. (n.d.). GossiTheDog@cyberplace.social. https://cyberplace.social/@GossiTheDog/111733024146282084
12. Hammond, A. (January 13, 2024). Welcome To 2024, The SSLVPN Chaos Continues - Ivanti CVE-2023-46805 & CVE-2024-21887. WatchTower Labs. https://labs.watchtowr.com/welcome-to-2024-the-sslvpn-chaos-continues-ivanti-cve-2023-46805-cve-2024-21887/

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

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