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.