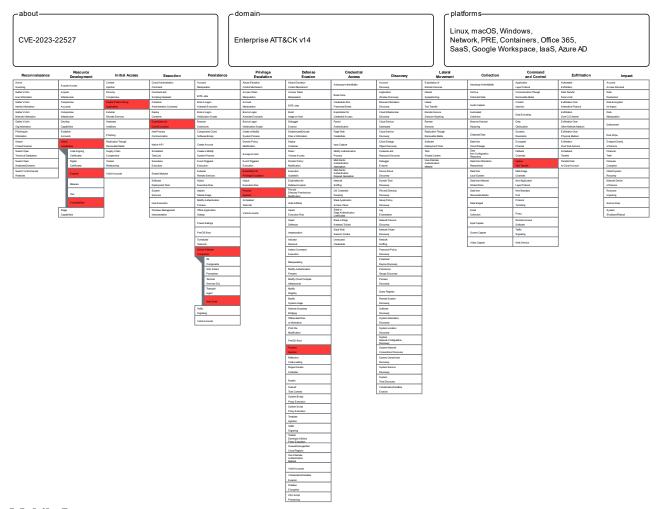
# MITRE ATT&CK Matrix - CVE-2023-22527 Atlassian Critical Vulnerabilities

## MITRE ATT&CK Matrix

## **Enterprise Layer**

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