

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

## 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

CVE-2023-22527

Enterprise ATT&amp;CK v14

Linux, macOS, Windows,  
Network, PRE, Containers, Office 365,  
SaaS, Google Workspace, IaaS, Azure AD

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