

CVE ACTIVELY EXPLOITED/ POC PUBLICLY AVAILABLE

Vulnerability	Affected Vendor/ Product	Vulnerability Type/ Component	Active Exploitation (POC Available)	Patch Available	Used in Ransomware campaign	Used by state actors
CVE-2023-20198	Cisco IOS XE Software	Web UI Privilege Escalation	Yes (Yes)	Yes	Not Known	Yes(Velvet Ant-China)
CVE-2023-51467	Apache OFBiz	Server-Side Request Forgery (SSRF)	Yes (Yes)	Yes	Not Known	Not Known
CVE-2023-36845	Juniper Networks Junos OS (EX Series and SRX Series)	PHP External Variable Modification	Yes (Yes)	Yes	Not Known	Not Known
CVE-2024-3400	Palo Alto Networks PAN-OS	Command Injection	Yes (Yes)	Yes	Not Known	Yes(Pioneer Kitten-Iran)
CVE-2022-22947	VMware Spring Cloud Gateway	Code Injection (Remote Code Execution)	Yes (Yes)	Yes	Not Known	Yes(Hafnium-China)
CVE-2023-22515	Atlassian Confluence Data Center and Server	Broken Access Control (Unauthenticated Remote Code Execution)	Yes (Yes)	Yes	Yes (Cerber Ransomware, Ransom Hub Ransomware)	Yes(Dark Shadow)
CVE-2023-20198	Cisco IOS XE Software	Web UI Privilege Escalation	Yes (Yes)	Yes	Not Known	Yes(Velvet Ant-China)
CVE-2020-11023	jQuery JavaScript library	Cross-Site Scripting (XSS)	Yes (Yes)	Yes	Not Known	Yes(APT41-China)
CVE-2025-23006	SonicWall SMA1000 Appliances	Pre-authentication Deserialization of Untrusted Data	Yes (No)	Yes	Not Known	Not Known