

CVE ACTIVELY EXPLOITED/ POC PUBLICLY AVAILABLE

CVE ID	Affected Vendor/ Product	Vulnerability Type/ Component	Active Exploitation (POC Available)	Patch Available	Used in Ransomware campaign	Used by state actors	Other Notable Activity Seen/ Reported
CVE-2024-51378	CyberPanel	An Incorrect Default Permissions vulnerability	Yes (Yes)	Yes	Yes(PSAUX, C3RB3R, Helldown.a nd Babuk Ransomware)	Unknown	
CVE-2024-49138	Microsoft Windows Common Log File System (CLFS) driver	Heap-based buffer overflow vulnerability	Yes (Yes)	Yes	Unknown	Unknown	This vulnerability could be leveraged using DDoS toolkits and rootkits.
CVE-2024-41713 CVE-2024-35286	Mitel MiCollab	Vulnerabilities could potentially allow unauthorized access to sensitive files	Yes (Yes)	Yes	Unknown	Unknown	
CVE-2024-11639	Ivanti Cloud Services Application	An Authentication Bypass Using an Alternate Path or Channel vulnerability	Yes (No)	Yes	Unknown	Unknown	
CVE-2024-11772	Ivanti Cloud Services Application	Command injection in the admin web console	Yes (No)	Yes	Unknown	Unknown	
CVE-2024-11773	Ivanti Cloud Services Application	SQL injection in the admin web console	Yes (No)	Yes	Unknown	Unknown	
CVE-2024-11972	WordPress Hunk Companion Plugin	It can be exploited for attacks such as Remote Code Execution (RCE), SQL Injection, Cross-Site Scripting	No (No)	No	Unknown	Unknown	

CVE ID	Affected Vendor/ Product	Vulnerability Type/ Component	Active Exploitation (POC Available)	Patch Available	Used in Ransomware campaign	Used by state actors	Other Notable Activity Seen/ Reported
		(XSS), or even the creation of administrative backdoors					