

CVE ACTIVELY EXPLOITED/ POC PUBLICLY AVAILABLE

Vulnerability	Affected Vendor/ Product	Vulnerability Type/ Component	Active Exploitation (POC Available)	Patch Available	Used in Ransomware campaign/State Actors Campaign
CVE-2023-48365	Qlik Sense	HTTP Request/Response Smuggling vulnerability	Yes (No)	Yes	Cactus ransomware group
CVE-2024-12686	BeyondTrust's Privileged Remote Access and Remote Support products	OS Command Injection vulnerability	Yes (No)	Yes	Unknown
CVE-2025-21335 CVE-2025-21334 CVE-2025-21333	Microsoft Windows Hyper-V platform	A Use After Free vulnerability	Yes (Yes)	Yes	Unknown
CVE-2024-55591	FortiOS and FortiProxy	Authentication bypass vulnerability	Yes (No)	Yes	Unknown
CVE-2024-50603	Aviatrix Controller	Code Execution vulnerability	Yes (Yes)	Yes	Unknown
CVE-2024-10811	Ivanti Endpoint Manager	An Absolute Path Traversal vulnerability	Yes (No)	Yes	Unknown
CVE-2024-13161 CVE-2024-13160 CVE-2024-13159	Ivanti Endpoint Manager	An Absolute Path Traversal vulnerability	Yes (No)	Yes	Unknown