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	Other Notable Activity Seen/Reported
CVE-2024-11667	Multiple Zyxel firewalls (ATP series firmware)	Path traversal vulnerability	Yes(No)	Yes	Yes (Helldown ransomware)	Unknown	
CVE-2024-11680	ProjectSend	Improper authentication vulnerability	Yes(Yes)	Yes	Unknown	Unknown	
CVE-2023-45727	North Grid Proself Enterprise/Standard, Gateway, and Mail Sanitize	Improper restriction of XML External Entity (XXE) reference vulnerability	yes(No)	Yes	Unknown	Earth Kasha	
CVE-2021-21206	Google Chromium Blink	Use-after-free vulnerability	Yes(Yes)	Yes	Unknown	Unknown	
CVE-2024-45216	Apache Solr	Authentication bypass vulnerability	yes(yes)	Yes	Unknown	Unknown	
CVE-2024-21287	Oracle Agile Product Lifecycle Management	Incorrect Authorization	Yes(No)	Yes	Unknown	Unknown	
CVE-2024-9474	Palo Alto PAN-OS	Improper Neutralization of Special Elements Used in an OS Command	yes(yes)	Yes	Unknown	Unknown	Exploited in “Operation Lunar Peek”
CVE-2024-0012	Palo Alto PAN-OS	Missing Authentication for Critical Function	yes(yes)	Yes	Unknown	Unknown	Exploited in “Operation Lunar Peek”

Vulnerability	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-2024-48860	QNAP QuRouter	Improper Neutralization of Special Elements Used in an OS Command	No(No)	yes	Unknown	Unknown	
CVE-2024-38645	QNAP Note Station 3	Server-Side Request Forgery (SSRF)	No(No)	yes	Unknown	Unknown	
CVE-2024-9478	Upkeeper Instant Privilege Access	Improper Privilege Management	No(No)	Yes	Unknown	Unknown	
CVE-2024-11145	Easy Folder Listing Pro	Deserialization of Untrusted Data	No(No)	Yes	Unknown	Unknown	
CVE-2024-47073	Data Ease	Improper Verification of Cryptographic Signature	No(No)	Yes	Unknown	Unknown	
CVE-2024-8074	Nomysem	Improper Privilege Management	No(No)	Yes	Unknown	Unknown	
CVE-2024-10934	OpenBSD	Double Free	No(No)	Yes	Unknown	Unknown	
CVE-2024-10218	TIBCO Operational Intelligence (TIBCO Hawk)	Improper Restriction of XML External Entity Reference	No(No)	Yes	Unknown	Unknown	
CVE-2024-5921	Palo Alto Networks GlobalProtect	Improper Certificate Validation	No(yes)	Yes	Unknown	Unknown	
CVE-2024-41992	Arcadyan FMIMG51AX000J	Improper Neutralization of Special Elements	No(yes)	No	Unknown	Unknown	

Vulnerability	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
		Used in an OS Command					
CVE-2024-11120	GeoVision Gvlx 4 V3, V2, Gv-Vs11, Gv-Dsp Lpr V3	Improper Neutralization of Special Elements Used in an OS Command	yes(no)	Yes	Unknown	Unknown	Threat actors use CVE-2024-11120 to enlist devices in the Mirai botnet in order to conduct cryptomining and DDoS attack.
CVE-2024-49019	Windows Active Directory Certificate Services	Weak Authentication	No(No)	Yes	Unknown	Unknown	
CVE-2024-52380	Picsmize Plugin	Unrestricted Upload of File with Dangerous Type	No(No)	No	Unknown	Unknown	
CVE-2024-10924	"Really Simple Security" WordPress plugin	Missing Authentication for Critical Function	No(No)	yes	Unknown	Unknown	
CVE-2024-48990	Needrestart Project	Uncontrolled Search Path Element	No(yes)	Yes	Unknown	Unknown	