

CVEs Used in Ransomware Campaigns: 2025 Manufacturing Report by Black Kite

CVE	Vendor	Product	Vulnerability Name	Ransomware Campaign Use
CVE-2023-24880	Microsoft	Windows	Microsoft Windows SmartScreen Security Feature Bypass Vulnerability	Known
CVE-2021-27065	Microsoft	Exchange Server	Microsoft Exchange Server Remote Code Execution Vulnerability	Known
CVE-2021-26857	Microsoft	Exchange Server	Microsoft Exchange Server Remote Code Execution Vulnerability	Known
CVE-2021-34473	Microsoft	Exchange Server	Microsoft Exchange Server Remote Code Execution Vulnerability	Known
CVE-2021-26858	Microsoft	Exchange Server	Microsoft Exchange Server Remote Code Execution Vulnerability	Known
CVE-2021-26855	Microsoft	Exchange Server	Microsoft Exchange Server Remote Code Execution Vulnerability	Known
CVE-2020-3259	Cisco	Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD)	Cisco ASA and FTD Information Disclosure Vulnerability	Known
CVE-2024-4577	PHP Group	PHP	PHP-CGI OS Command Injection Vulnerability	Known
CVE-2023-4966	Citrix	NetScaler ADC and NetScaler Gateway	Citrix NetScaler ADC and NetScaler Gateway Buffer Overflow Vulnerability	Known
CVE-2023-3519	Citrix	NetScaler ADC and NetScaler Gateway	Citrix NetScaler ADC and NetScaler Gateway Code Injection Vulnerability	Known
CVE-2023-22527	Atlassian	Confluence Data Center and Server	Atlassian Confluence Data Center and Server Template Injection Vulnerability	Known
CVE-2023-22518	Atlassian	Confluence Data Center and Server	Atlassian Confluence Data Center and Server Improper Authorization Vulnerability	Known
CVE-2021-36942	Microsoft	Windows	Microsoft Windows Local Security Authority (LSA) Spoofing Vulnerability	Known
CVE-2023-42793	JetBrains	TeamCity	JetBrains TeamCity Authentication Bypass Vulnerability	Known
CVE-2024-37085	VMware	ESXi	VMware ESXi Authentication Bypass Vulnerability	Known
CVE-2019-11043	PHP	FastCGI Process Manager (FPM)	PHP FastCGI Process Manager (FPM) Buffer Overflow Vulnerability	Known
CVE-2024-1709	ConnectWise	ScreenConnect	ConnectWise ScreenConnect Authentication Bypass Vulnerability	Known
CVE-2024-38475	Apache	HTTP Server	Apache HTTP Server Improper Escaping of Output Vulnerability	Unknown
CVE-2024-29059	Microsoft	.NET Framework	Microsoft .NET Framework Information Disclosure Vulnerability	Unknown
CVE-2023-44487	IETF	HTTP/2	HTTP/2 Rapid Reset Attack Vulnerability	Unknown
CVE-2025-24984	Microsoft	Windows	Microsoft Windows NTFS Information Disclosure Vulnerability	Unknown
CVE-2024-21413	Microsoft	Office Outlook	Microsoft Outlook Improper Input Validation Vulnerability	Unknown
CVE-2021-31196	Microsoft	Exchange Server	Microsoft Exchange Server Information Disclosure Vulnerability	Unknown
CVE-2024-3400	Palo Alto Networks	PAN-OS	Palo Alto Networks PAN-OS Command Injection Vulnerability	Unknown
CVE-2025-33053	Web Distributed Authoring and Versioning	Web Distributed Authoring and Versioning (WebDAV)	Web Distributed Authoring and Versioning (WebDAV) External Control of File Name or Path Vulnerability	Unknown
CVE-2025-32706	Microsoft	Windows	Microsoft Windows Common Log File System (CLFS) Driver Heap-Based Buffer Overflow Vulnerability	Unknown
CVE-2025-32701	Microsoft	Windows	Microsoft Windows Common Log File System (CLFS) Driver Use-After-Free Vulnerability	Unknown
CVE-2025-30397	Microsoft	Windows	Microsoft Windows Scripting Engine Type Confusion Vulnerability	Unknown
CVE-2025-24054	Microsoft	Windows	Microsoft Windows NTLM Hash Disclosure Spoofing Vulnerability	Unknown
CVE-2025-29824	Microsoft	Windows	Microsoft Windows Common Log File System (CLFS) Driver Use-After-Free Vulnerability	Unknown
CVE-2025-26633	Microsoft	Windows	Microsoft Windows Management Console (MMC) Improper Neutralization Vulnerability	Unknown
CVE-2025-24991	Microsoft	Windows	Microsoft Windows NTFS Out-Of-Bounds Read Vulnerability	Unknown
CVE-2025-24983	Microsoft	Windows	Microsoft Windows Win32k Use-After-Free Vulnerability	Unknown
CVE-2025-24993	Microsoft	Windows	Microsoft Windows NTFS Heap-Based Buffer Overflow Vulnerability	Unknown
CVE-2015-2360	Microsoft	Win32k	Microsoft Win32k Privilege Escalation Vulnerability	Unknown
CVE-2015-2387	Microsoft	ATM Font Driver	Microsoft ATM Font Driver Privilege Escalation Vulnerability	Unknown
CVE-2017-7269	Microsoft	Internet Information Services (IIS)	Microsoft Windows Server Buffer Overflow Vulnerability	Unknown
CVE-2025-22457	Ivanti	Connect Secure, Policy Secure and ZTA Gateways	Ivanti Connect Secure, Policy Secure and ZTA Gateways Stack-Based Buffer Overflow Vulnerability	Unknown
CVE-2025-0282	Ivanti	Connect Secure, Policy Secure, and ZTA Gateways	Ivanti Connect Secure, Policy Secure, and ZTA Gateways Stack-Based Buffer Overflow Vulnerability	Unknown
CVE-2024-21893	Ivanti	Connect Secure, Policy Secure, and Neurons	Ivanti Connect Secure, Policy Secure, and Neurons Server-Side Request Forgery (SSRF) Vulnerability	Unknown
CVE-2024-21887	Ivanti	Connect Secure and Policy Secure	Ivanti Connect Secure and Policy Secure Command Injection Vulnerability	Unknown
CVE-2023-46805	Ivanti	Connect Secure and Policy Secure	Ivanti Connect Secure and Policy Secure Authentication Bypass Vulnerability	Unknown
CVE-2024-20353	Cisco	Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD)	Cisco ASA and FTD Denial of Service Vulnerability	Unknown
CVE-2024-20359	Cisco	Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD)	Cisco ASA and FTD Privilege Escalation Vulnerability	Unknown
CVE-2023-6549	Citrix	NetScaler ADC and NetScaler Gateway	Citrix NetScaler ADC and NetScaler Gateway Buffer Overflow Vulnerability	Unknown
CVE-2024-21410	Microsoft	Exchange Server	Microsoft Exchange Server Privilege Escalation Vulnerability	Unknown
CVE-2024-38094	Microsoft	SharePoint	Microsoft SharePoint Deserialization Vulnerability	Unknown
CVE-2024-28995	SolarWinds	Serv-U	SolarWinds Serv-U Path Traversal Vulnerability	Unknown
CVE-2023-23752	Joomla	Joomla	Joomla! Improper Access Control Vulnerability	Unknown
CVE-2024-47575	Fortinet	FortiManager	Fortinet FortiManager Missing Authentication Vulnerability	Unknown
CVE-2024-23113	Fortinet	Multiple Products	Fortinet Multiple Products Format String Vulnerability	Unknown
CVE-2024-43573	Microsoft	Windows	Microsoft Windows MSHTML Platform Spoofing Vulnerability	Unknown
CVE-2024-43461	Microsoft	Windows	Microsoft Windows MSHTML Platform Spoofing Vulnerability	Unknown
CVE-2024-38112	Microsoft	Windows	Microsoft Windows MSHTML Platform Spoofing Vulnerability	Unknown
CVE-2025-31324	SAP	NetWeaver	SAP NetWeaver Unrestricted File Upload Vulnerability	Unknown
CVE-2023-44487	IETF	HTTP/2	HTTP/2 Rapid Reset Attack Vulnerability	Unknown
CVE-2025-4428	Ivanti	Endpoint Manager Mobile (EPMM)	Ivanti Endpoint Manager Mobile (EPMM) Code Injection Vulnerability	Unknown
CVE-2025-4427	Ivanti	Endpoint Manager Mobile (EPMM)	Ivanti Endpoint Manager Mobile (EPMM) Authentication Bypass Vulnerability	Unknown
CVE-2020-2883	Oracle	WebLogic Server	Oracle WebLogic Server Unspecified Vulnerability	Unknown
CVE-2017-3506	Oracle	WebLogic Server	Oracle WebLogic Server OS Command Injection Vulnerability	Unknown
CVE-2020-2551	Oracle	Fusion Middleware	Oracle Fusion Middleware Unspecified Vulnerability	Unknown
CVE-2017-12637	SAP	NetWeaver	SAP NetWeaver Directory Traversal Vulnerability	Unknown
CVE-2025-21590	Juniper	Junos OS	Juniper Junos OS Improper Isolation or Compartmentalization Vulnerability	Unknown
CVE-2024-21762	Fortinet	FortiOS	Fortinet FortiOS Out-of-Bound Write Vulnerability	Unknown
CVE-2023-27997	Fortinet	FortiOS and FortiProxy SSL-VPN	Fortinet FortiOS and FortiProxy SSL-VPN Heap-Based Buffer Overflow Vulnerability	Unknown
CVE-2022-42475	Fortinet	FortiOS	Fortinet FortiOS Heap-Based Buffer Overflow Vulnerability	Unknown
CVE-2025-42999	SAP	NetWeaver	SAP NetWeaver Deserialization Vulnerability	Unknown
CVE-2019-0344	SAP	Commerce Cloud	SAP Commerce Cloud Deserialization of Untrusted Data Vulnerability	Unknown
CVE-2024-4885	Progress	WhatsUp Gold	Progress WhatsUp Gold Path Traversal Vulnerability	Unknown
CVE-2024-6670	Progress	WhatsUp Gold	Progress WhatsUp Gold SQL Injection Vulnerability	Unknown
CVE-2024-23897	Jenkins	Jenkins Command Line Interface (CLI)	Jenkins Command Line Interface (CLI) Path Traversal Vulnerability	Unknown
CVE-2024-4040	CrushFTP	CrushFTP	CrushFTP VFS Sandbox Escape Vulnerability	Unknown
CVE-2022-26904	Microsoft	Windows	Microsoft Windows User Profile Service Privilege Escalation Vulnerability	Unknown
CVE-2025-24813	Apache	Tomcat	Apache Tomcat Path Equivalence Vulnerability	Unknown
CVE-2023-27524	Apache	Superset	Apache Superset Insecure Default Initialization of Resource Vulnerability	Unknown
CVE-2023-21839	Oracle	WebLogic Server	Oracle WebLogic Server Unspecified Vulnerability	Unknown
CVE-2024-42009	Roundcube	Webmail	RoundCube Webmail Cross-Site Scripting Vulnerability	Unknown
CVE-2024-37383	Roundcube	Webmail	RoundCube Webmail Cross-Site Scripting (XSS) Vulnerability	Unknown
CVE-2023-43770	Roundcube	Webmail	Roundcube Webmail Persistent Cross-Site Scripting (XSS) Vulnerability	Unknown
CVE-2023-5631	Roundcube	Webmail	Roundcube Webmail Persistent Cross-Site Scripting (XSS) Vulnerability	Unknown
CVE-2024-24919	Check Point	Quantum Security Gateways	Check Point Quantum Security Gateways Information Disclosure Vulnerability	Unknown
CVE-2024-27198	JetBrains	TeamCity	JetBrains TeamCity Authentication Bypass Vulnerability	Unknown
CVE-2021-26086	Atlassian	Jira Server and Data Center	Atlassian Jira Server and Data Center Path Traversal Vulnerability	Unknown
CVE-2025-23006	SonicWall	SMA1000 Appliances	SonicWall SMA1000 Appliances Deserialization Vulnerability	Unknown
CVE-2025-22225	VMware	ESXi	VMware ESXi Arbitrary Write Vulnerability	Unknown
CVE-2025-22224	VMware	ESXi and Workstation	VMware ESXi and Workstation TOCTOU Race Condition Vulnerability	Unknown
CVE-2025-22226	VMware	ESXi, Workstation, and Fusion	VMware ESXi, Workstation, and Fusion Information Disclosure Vulnerability	Unknown
CVE-2019-9621	Synacor	Zimbra Collaboration Suite (ZCS)	Synacor Zimbra Collaboration Suite (ZCS) Server-Side Request Forgery (SSRF) Vulnerability	Unknown
CVE-2024-11182	MDaemon	Email Server	MDaemon Email Server Cross-Site Scripting (XSS) Vulnerability	Unknown
CVE-2023-34192	Synacor	Zimbra Collaboration Suite (ZCS)	Synacor Zimbra Collaboration Suite (ZCS) Cross-Site Scripting (XSS) Vulnerability	Unknown
CVE-2024-45519	Synacor	Zimbra Collaboration	Synacor Zimbra Collaboration Command Execution Vulnerability	Unknown
CVE-2021-33044	Dahua	IP Camera Firmware	Dahua IP Camera Authentication Bypass Vulnerability	Unknown
CVE-2021-33045	Dahua	IP Camera Firmware	Dahua IP Camera Authentication Bypass Vulnerability	Unknown
CVE-2025-47812	Wing FTP Server	Wing FTP Server	Wing FTP Server Improper Neutralization of Null Byte or NUL Character Vulnerability	Unknown
CVE-2014-0497	Adobe	Flash Player	Adobe Flash Player Integer Underflow Vulnerability	Unknown
CVE-2014-0502	Adobe	Flash Player	Adobe Flash Player Double Free Vulnerability	Unknown
CVE-2013-0643	Adobe	Flash Player	Adobe Flash Player Incorrect Default Permissions Vulnerability	Unknown
CVE-2013-0648	Adobe	Flash Player	Adobe Flash Player Code Execution Vulnerability	Unknown
CVE-2024-4879	ServiceNow	Utah, Vancouver, and Washington DC Now	ServiceNow Improper Input Validation Vulnerability	Unknown
CVE-2024-5217	ServiceNow	Utah, Vancouver, and Washington DC Now	ServiceNow Incomplete List of Disallowed Inputs Vulnerability	Unknown
CVE-2024-27443	Synacor	Zimbra Collaboration Suite (ZCS)	Synacor Zimbra Collaboration Suite (ZCS) Cross-Site Scripting (XSS) Vulnerability	Unknown
CVE-2021-35247	SolarWinds	Serv-U	SolarWinds Serv-U Improper Input Validation Vulnerability	Unknown