INDIA

RANSOMWARE REPORT

YEAR 2024

Handling Computer Security Incidents

Preface

In the year 2024, the ransomware landscape has undergone a dramatic evolution, with threat actors deploying increasingly sophisticated tactics to target organizations of every size—from global enterprises to small and medium-sized businesses. The ecosystem has advanced substantially, with attackers refining their methods to accelerate attack velocity and maximize impact through meticulously coordinated operations.

Ransomware operators are now pivoting toward multi-faceted extortion strategies that blend data encryption, data exfiltration, and reputational threats with customized pressure tactics, compelling victims to pay ransoms. Notably, hacktivists and state-sponsored groups are also harnessing ransomware as a tool to further their illicit, financial and political agendas.

A particularly alarming trend in 2024 is the heightened targeting of virtualized environments in data centers, especially VMware ESXi hypervisors, which enables the Ransomware adversaries to encrypt entire fleets of virtual machines in a single, devastating move.

Despite the implementation of standard security tools, ongoing gaps in access control mechanisms, patch management, and monitoring processes continue to leave organizations vulnerable to ransomware threats, increasing the risk of exploitation.

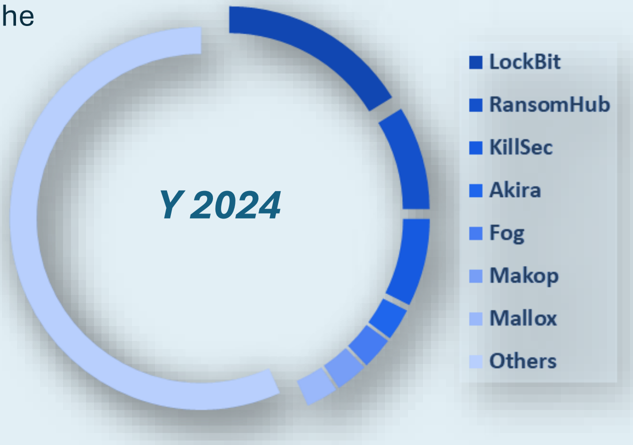
Human-operated ransomware attacks often leveraging living-off-the-land techniques and the legitimate IT tools to bypass traditional defenses and for lateral movements inside the compromised victim network.

While law enforcement agencies around the globe are intensifying their efforts to combat these threats, the financial incentives driving ransomware remain robust. Newer ransomware variants are emerging due to rebranding, regrouping, and the reuse of leaked malware code — further complicating the threat landscape.

This present report provides an analysis of the ransomware trend insights observed in the year 2024 along with known vulnerabilities exploited by Ransomware groups to help originations to strengthen their Ransomware resilience.

Ransomware - Trends

In 2024, LockBit, RansomHub and KillSec were the dominant ransomware groups impacting the Indian cyberspace. Year 2024 witnessed the emergence of many new ransomware variants, some of which exhibited unknown affiliations, suggesting the involvement of low-profile operators.



Ransomware Groups - Major Observations

LockBit maintained its position as the most active ransomware group in the year 2024. The availability of leaked LockBit Ransomware source code has also likely contributed to the proliferation of ransomware attacks by new players and affiliates.

RansomHub has emerged as a significant threat group, particularly targeting data center virtualization environments. Several organizations have experienced consecutive ransomware attacks, with RansomHub identified as one of the perpetrators. This pattern suggests potential collaboration or overlap between RansomHub's Ransomware-as-a-Service (RaaS) affiliates and other ransomware groups.

Hacktivist group KillSec has shifted its focus to ransomware operations, primarily exploiting public cloud storage misconfigurations, weak IAM policies and compromised credentials. In the observed cases, KillSec did not deploy ransom notes within affected infrastructures. Instead, exfiltrated data is directly advertised on their leak site for potential buyers, indicating a shift toward monetization through data sales.

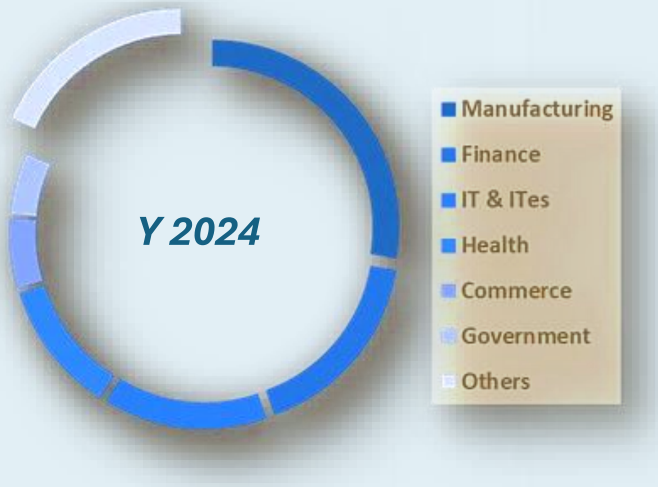
Makop primarily relied on exposed Remote Desktop Protocol (RDP) services for initial access, utilizing brute-force attacks and credential stuffing techniques to infiltrate networks. Organizations with unsecured RDP endpoints remain at high risk with Makop group.

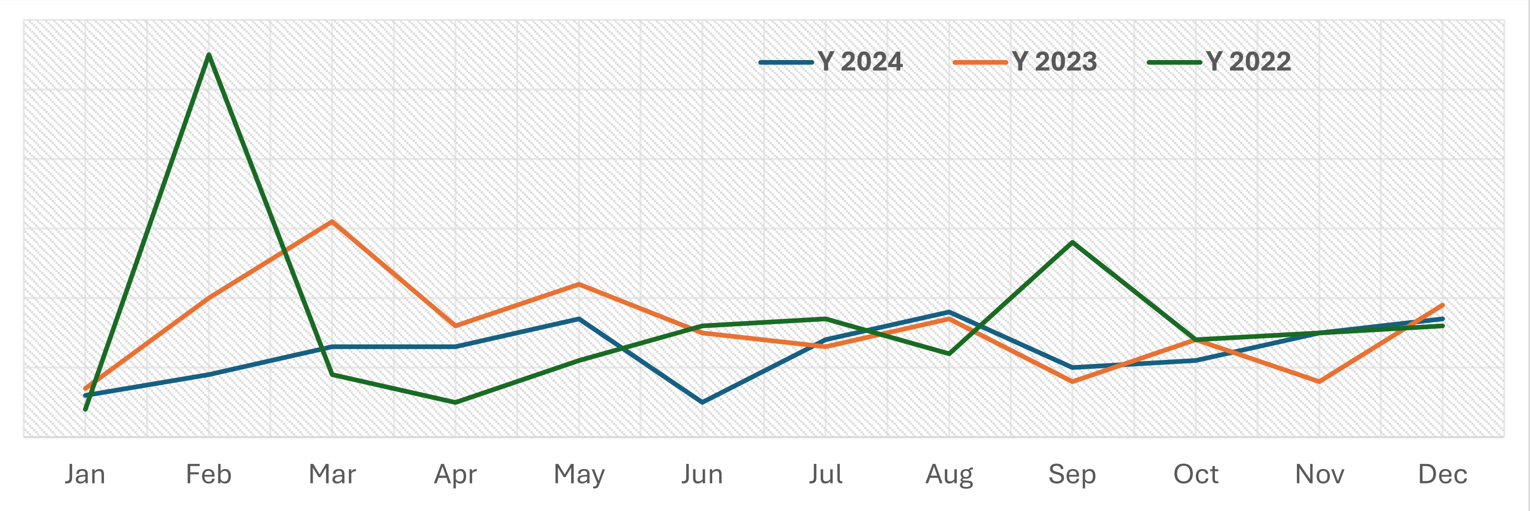
Mallox variant majorly targeted publicly exposed Microsoft SQL (MS-SQL) servers, using brute-force attacks to gain unauthorized access. Once inside, they deploy ransomware payloads, disrupt operations, and exfiltrate sensitive data for double extortion schemes.

Ransomware - Trends

In 2024, the Manufacturing sector was the most targeted by Ransomware attacks, followed closely by the Finance and IT & ITes sectors.

Ransomware actors are increasingly targeting public cloud infrastructure and have expanded their tactics to monetize attacks by compromising websites as well.





Ransomware Incidents Handled - Y 2024 *vs* Y 2023 *vs* Y 2022

Ransomware - Living off the Land techniques

In recent cases, CERT-In has identified a substantial rise in the abuse of Living off the Land Binaries and Scripts (LOLBAS) by nearly all ransomware groups. Threat actors are exploiting legitimate tools and operating system native binaries, such as PowerShell and Command Prompt to conduct malicious activities. The stealthy use of these tools poses significant challenges to security teams, as their presence is often deemed legitimate and routine in their enterprise environments.

PowerShell remains the preferred tool for ransomware operators. Its robust scripting capabilities allow attackers to remotely download and execute arbitrary code and binaries. Additionally, the use of encrypted and obfuscated scripts further complicates efforts to identify and mitigate PowerShell based threats. By abusing PowerShell, ransomware groups can establish persistence within compromised systems, execute lateral movement, and perform other critical functions necessary for subsequent attack stages.

In addition to PowerShell, ransomware actors are relying on command prompt-based commands and batch scripts to perform reconnaissance, manipulate critical registry entries, and disable or bypass local security controls at the system level. Through batch scripts, adversaries can automate tasks such as privilege escalation, system configuration changes, and the disabling of endpoint protections, thereby laying the groundwork for more devastating attack stages.

Furthermore, ransomware actors are increasingly leveraging the “Bring Your Own Vulnerable Driver (BYOVD)” technique, implanting legitimate yet vulnerable drivers into the targeted system allowing attackers to bypass security measures, escalate privileges to kernel level, and disable endpoint defenses.

Remote Monitoring and Management (RMM) tools such as AnyDesk, ScreenConnect, Splashtop are being abused maintain access and control, setting the stage for a ransomware attack in victim environments.

For detailed insights on identifying and mitigating Living Off the Land techniques, refer to the resources available at *https://lolol.farm* and Joint Guidance on “Identifying and Mitigating Living Off the Land Techniques” available at URL: “https://www.cisa.gov/sites/default/files/2025-03/Joint-Guidance-Identifying-and-Mitigating-LOTL508.pdf”

Ransomware Target - Exposed services

CERT-In has observed a significant surge in ransomware attacks targeting internet-exposed database instances, ESXi servers, and NAS devices in 2024. Mallox ransomware group has been particularly active, exploiting publicly accessible MS SQL instances through brute-force attacks. Once access is gained, attackers leverage “xp_cmdshell” to execute PowerShell scripts, deploy ransomware, and encrypt critical data.

Additionally, ransomware campaigns have targeted publicly exposed NAS devices and Redis servers, further escalating the threat landscape.

Internet-facing VMware ESXi hypervisors with vulnerabilities CVE-2021-21974, CVE-2020-3992, and CVE-2019-5544 have also been actively exploited by threat actors to launch ransomware attacks.

Also, many organizations are exposing their firewall management consoles to the internet leading to risk associated with exploitation of those instances.

It is essential to regularly review the public facing assets and apply necessary patches and access restrictions to prevent exploitation. Organizations can onboard the Cyber Swachhta Kendra (csk.gov.in) platform and CERT-In’s Malware Threat eXchange (CMTX) platform to avail actionable threat intelligence in this aspect.

As part of proactive mitigation efforts, CERT-In conducted a comprehensive assessment, identifying thousands of vulnerable ESXi and MS SQL instances. Advisories were issued to infrastructure owners, accompanied by tailored remedial measures to mitigate risks and enhance their infrastructure security.

Hypervisor layer attacks

Ransomware actors are increasingly targeting virtualization infrastructure, with a concentrated focus on hypervisor layers in VMware ESXi environments. Though attacks on Hyper-V based systems have also visible in the year 2024, VMware ESXi remains a primary target due to its widespread enterprise adoption and inherent security limitations, such as the lack of native support for antivirus (AV) or endpoint detection and response (EDR). The VMware hypervisor layer is frequently overlooked by security teams, leading to undetected threat activity by Ransomware actors. This gap is allowing attackers to deploy ransomware encryptors directly onto the hypervisor, compromising all associated virtual machines (VMs) in a single strike.

Attackers often exploit poorly secured vCenter management consoles, leveraging weak access restrictions to enable SSH services on ESXi instances. Once SSH access is established, ransomware payloads are getting deployed to encrypt VM files. Threat actors are also utilizing SSH tunneling as a persistence mechanism.

It is important to centralize the logs of ESXi (including critical sources such as auth.log, shell.log, hostd.log, vobd.log) and vCenter services with alerting mechanisms for detecting any suspicious events. Network segmentation with restricted access to VMware management interfaces is essential to reduce the risk of infections.

Ransomware Defense Evasion

A significant rise in the utilization of EDR (Endpoint Detection and Response) evasion tools by ransomware actors has been observed, highlighting an evolving threat landscape. Threat groups are increasingly leveraging EDR killers, blockers, and silencers to disable or bypass endpoint security solutions to facilitate ransomware deployment.

These cyber threat actors have leveraged anti-rootkit applications, exploited vulnerable drivers, and utilized various utility tools to bypass and manipulate host-level defenses. Additionally, they have been observed remotely executing ransomware payloads without writing them to disk, making detection and mitigation by EDR solutions significantly more challenging.

Furthermore, a concerning trend of over-reliance on security tools without proper logging and monitoring has been observed, leaving organizations vulnerable to ransomware threats. Ineffective alert management—such as failing to monitor security alerts and analyze logs—has significantly contributed to prolonged ransomware infections and deeper intrusions.

Commonly observed tools for EDR evasion include:

- EDRSilencer
- AuKill
- EDRKillShifter
- TDSSkiller
- HRSWord
- GMER
- Process Hacker
- IOBit Uninstaller

In addition to using tool-based evasion tactics, ransomware operators frequently manipulate host-level configurations to further evade detection and enhance their attack persistence. These include:

- Host Firewall Modifications: Altering firewall rules to enable inbound Remote Desktop Protocol (RDP) connections, facilitating unauthorized remote access.
- Registry-Level Changes: Using command-line scripts and batch files to modify registry settings, weakening host-level defense mechanisms.
- In some instances, Endpoint Detection and Response (EDR) agents have been uninstalled through the Windows Task Manager, further compromising security defenses.

Ransomware BitLocker encryptions

Ransomware groups are increasingly exploiting BitLocker, a native Windows encryption feature, to lock victims out of their systems. Unlike traditional ransomware that encrypts individual files, this technique encrypts entire drives, significantly complicating recovery efforts

Threat actors often gain initial access through exposed RDP services. Once inside, they conduct reconnaissance, use remote access tools for persistence, and execute commands via Windows shell utilities.

Before enabling BitLocker through PowerShell or Group Policy, attackers may exfiltrate data to various cloud storage services. They frequently abuse the "manage-bde.exe" binary to facilitate BitLocker device encryption. To further hinder recovery, attackers may force system shutdowns, making data restoration even more challenging.

Ransomware – System lockouts

Ransomware attacks are evolving beyond traditional file encryption to include system lockouts, where attackers manipulate login credentials and system access to further extort victims. Instead of merely encrypting data, threat actors alter existing credentials, disable administrative accounts, and create rogue user accounts with elevated privileges. This prevents legitimate users from accessing their own systems, effectively locking them out.

Attackers modify system settings to display the ransom note message on infected machines using the Windows Legal Notice and Linux Message of the Day (MOTD) features, ensuring that ransom demands appear at the system login screen.

In some cases, attackers demand a separate ransom for providing access to locked system, thus paving the way for partial monetization of Ransom amount.

Fake Ransomware campaigns

Ransomware groups are increasingly employing deceptive tactics to pressure victims into paying ransoms, even when no actual data exfiltration or attack has occurred. These strategies reflect the growing sophistication of threat activities and the increasing complexity of the threat landscape.

Groups like Basche are sourcing previously breached data or creating fabricated datasets to display on their data leak sites, falsely claiming an attack to extort ransom payments. They may also offer the alleged data for sale, coercing victims into paying under the false belief that their information has been compromised—even when no breach has actually taken place by that particular campaign.

Some ransomware variants wipe data from infected hosts while falsely claiming to have exfiltrated it. These deceptive claims are especially prevalent in attacks on public cloud environments, where attackers exploit cloud complexity to obscure their activities. Victims are manipulated into paying ransoms to "retrieve" data that was never actually stolen.

In cases where victims negotiate and pay ransoms based on these fabricated claims, attackers often become unresponsive, leaving victims with both data loss and monetary loss.

The rise of fake ransomware claims and fabricated data leaks underscores the increasing psychological manipulation tactics used by ransomware groups. By exploiting fear and reputational damage, these groups pressure victims into unnecessary payments. Organizations must remain vigilant, adopt evidence-based approaches to verify extortion claims, and avoid falling victim to these deceptive strategies.

Customized Extortion campaigns

Ransomware attackers are increasingly adopting customized extortion techniques, employing aggressive and highly personalized methods to coerce victims into paying ransoms.

Rather than relying solely on ransom notes or messages, attackers now use direct outreach, including phone calls and targeted emails to key stakeholders. One of their primary tactics involves sending emails and making personalized calls via virtual numbers, targeting senior executives, associates, and IT administrators of the victim organization. Attackers directly pressure these individuals with threats of re-attacks, data exposure, and breach disclosures to clients and regulatory bodies, heightening the urgency to comply with ransom demands.

When ransom demands remain unmet, some attackers escalate their tactics by sending preemptive emails to regulatory authorities, alleging non-compliance and data protection failures by the victim entity.

Consecutive Ransomware Attacks

There has been a rise in cases where victims experience consecutive ransomware attacks from different groups. Due to incomplete remediation efforts, attackers are re-exploiting unpatched vulnerabilities and persistent backdoors, allowing them to target the same organization.

Additionally, victim cross-claims have been observed on some data leak sites, where multiple ransomware groups claim responsibility for the same attack. Notably, in incidents where multiple ransomware infections were reported by the victim, RansomHub was one of the variants, suggesting possible overlapping or coordinated operations between RansomHub RaaS affiliates and other threat groups.

Convergence of Hacktivism and Ransomware

Hacktivism has evolved from digital protest into a complex cyber threat landscape, where some groups now leverage ransomware for financial gain or ideological influence. While traditional hacktivists focused on website defacement and DDoS attacks, some have transitioned to using ransomware tools, launching ransomware-as-a-service (RaaS) platforms, or collaborating with cyber threat actor groups.

This shift has been further fueled by geopolitical and religious conflicts, politicizing cyber threats and giving rise to hybrid groups that operate at the intersection of activism, state-sponsored cyber operations, and profit-driven operations.

A notable example is KillSec, a hacktivist group that recently launched its own RaaS platform, demonstrating how these groups are increasingly merging political motives with financially motivated malicious cyber operations.

Hacktivist-ransomware collaborations are on the rise, with shared tools, overlapping victims, and financial incentives driving these evolving alliances.

Ransomware – List of Vulnerabilities exploited

The list of known vulnerabilities exploited by various ransomware groups categorized by vendor and product:

CVE Number	Vendor - Product
CVE-2021-27104	Accellion-FTA
CVE-2021-27102	Accellion-FTA
CVE-2021-27101	Accellion-FTA
CVE-2021-27103	Accellion-FTA
CVE-2009-3960	Adobe-BlazeDS
CVE-2023-29300	Adobe-ColdFusion
CVE-2023-38203	Adobe-ColdFusion
CVE-2010-2861	Adobe-ColdFusion
CVE-2016-1019	Adobe-Flash Player
CVE-2018-15982	Adobe-Flash Player
CVE-2018-4878	Adobe-Flash Player
CVE-2010-0188	Adobe-Reader and Acrobat
CVE-2023-46604	Apache-ActiveMQ
CVE-2021-42013	Apache-HTTP Server
CVE-2021-41773	Apache-HTTP Server
CVE-2021-45046	Apache-Log4j2
CVE-2021-44228	Apache-Log4j2
CVE-2021-45105	Apache-Log4j2
CVE-2017-5638	Apache-Struts
CVE-2017-12615	Apache-Tomcat
CVE-2023-28461	Array Networks -AG/vxAG ArrayOS
CVE-2023-22527	Atlassian-Confluence Data Center and Server
CVE-2023-22518	Atlassian-Confluence Data Center and Server
CVE-2023-22515	Atlassian-Confluence Data Center and Server
CVE-2021-26085	Atlassian-Confluence Server
CVE-2021-26084	Atlassian-Confluence Server and Data Center
CVE-2019-3396	Atlassian-Confluence Server and Data Server
CVE-2022-26134	Atlassian-Confluence Server/Data Center
CVE-2021-42258	BQE-BillQuick Web Suite
CVE-2024-24919	Check Point-Quantum Security Gateways
CVE-2020-3259	Cisco-Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD)
CVE-2020-3580	Cisco-Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD)
CVE-2023-20269	Cisco-Adaptive Security Appliance and Firepower Threat Defense
CVE-2020-3433	Cisco-AnyConnect Secure
CVE-2020-3153	Cisco-AnyConnect Secure
CVE-2020-8195	Citrix
CVE-2020-8196	Citrix
CVE-2019-19781	Citrix
CVE-2019-11634	Citrix

CVE-2022-27510	Citrix
CVE-2019-19781	Citrix-Application Delivery Controller (ADC), Gateway, and SD-WAN WANOP
CVE-2023-4966	Citrix-NetScaler ADC and NetScaler Gateway
CVE-2023-3519	Citrix-NetScaler ADC and NetScaler Gateway
CVE-2021-22941	Citrix-ShareFile
CVE-2019-13608	Citrix-StoreFront Server
CVE-2019-11634	Citrix-Workspace Application and Receiver for Windows
CVE-2024-55956	Cleo-Multiple Products
CVE-2024-50623	Cleo-Multiple Products
CVE-2024-1709	ConnectWise-ScreenConnect
CVE-2024-51378	CyberPersons-CyberPanel
CVE-2018-10562	Dasan-Gigabit Passive Optical Network (GPON) Routers
CVE-2019-16057	D-Link-DNS-320 Storage Device
CVE-2018-6530	D-Link-Multiple Routers
CVE-2022-26352	dotCMS-dotCMS
CVE-2017-9822	DotNetNuke (DNN)-DotNetNuke (DNN)
CVE-2018-7602	Drupal-Core
CVE-2018-7600	Drupal-Drupal Core
CVE-2018-6789	Exim-Exim
CVE-2022-1388	F5-BIG-IP
CVE-2020-5902	F5-BIG-IP
CVE-2021-22986	F5-BIG-IP and BIG-IQ Centralized Management
CVE-2023-46747	F5-BIG-IP Configuration Utility
CVE-2021-35464	ForgeRock-Access Management (AM)
CVE-2023-48788	Fortinet-FortiClient EMS
CVE-2020-12812	Fortinet-FortiOS
CVE-2019-5591	Fortinet-FortiOS
CVE-2018-13379	Fortinet-FortiOS
CVE-2022-42475	Fortinet-FortiOS
CVE-2018-13374	Fortinet-FortiOS and FortiADC
CVE-2024-55591	Fortinet-FortiOS and FortiProxy
CVE-2018-13382	Fortinet-FortiOS and FortiProxy
CVE-2018-13383	Fortinet-FortiOS and FortiProxy
CVE-2023-27997	Fortinet-FortiOS and FortiProxy SSL-VPN
CVE-2022-40684	Fortinet-Multiple Products
CVE-2023-0669	Fortra-GoAnywhere MFT
CVE-2018-19323	GIGABYTE-Multiple Products
CVE-2018-19322	GIGABYTE-Multiple Products
CVE-2018-19321	GIGABYTE-Multiple Products
CVE-2018-19320	GIGABYTE-Multiple Products
CVE-2022-47986	IBM-Aspera Faspex
CVE-2013-3993	IBM-InfoSphere BigInsights
CVE-2023-35078	Ivanti-Endpoint Manager Mobile (EPMM)
CVE-2023-35082	Ivanti-Endpoint Manager Mobile (EPMM) and MobileIron Core
CVE-2021-22893	Ivanti-Pulse Connect Secure

CVE-2020-8260	Ivanti-Pulse Connect Secure
CVE-2020-8243	Ivanti-Pulse Connect Secure
CVE-2019-11539	Ivanti-Pulse Connect Secure
CVE-2019-11510	Ivanti-Pulse Connect Secure
CVE-2019-11539	Ivanti-Pulse Connect Secure and Pulse Policy Secure
CVE-2023-38035	Ivanti-Sentry
CVE-2024-23897	Jenkins-Jenkins Command Line Interface (CLI)
CVE-2024-27198	JetBrains-TeamCity
CVE-2023-42793	JetBrains-TeamCity
CVE-2017-18362	Kaseya-Virtual System/Server Administrator (VSA)
CVE-2018-20753	Kaseya-Virtual System/Server Administrator (VSA)
CVE-2021-30116	Kaseya-Virtual System/Server Administrator (VSA)
CVE-2021-3129	Laravel-Ignition
CVE-2017-1000253	Linux-Kernel
CVE-2021-42287	Microsoft-Active Directory
CVE-2021-42278	Microsoft-Active Directory
CVE-2016-0151	Microsoft-Client-Server Run-time Subsystem (CSRSS)
CVE-2022-44698	Microsoft-Defender
CVE-2018-8406	Microsoft-DirectX Graphics Kernel (DXGKRNL)
CVE-2018-8405	Microsoft-DirectX Graphics Kernel (DXGKRNL)
CVE-2020-0878	Microsoft-Edge and Internet Explorer
CVE-2021-42321	Microsoft-Exchange
CVE-2022-41080	Microsoft-Exchange Server
CVE-2022-41082	Microsoft-Exchange Server
CVE-2022-41040	Microsoft-Exchange Server
CVE-2018-8581	Microsoft-Exchange Server
CVE-2021-34523	Microsoft-Exchange Server
CVE-2020-0688	Microsoft-Exchange Server
CVE-2021-34473	Microsoft-Exchange Server
CVE-2021-31207	Microsoft-Exchange Server
CVE-2021-26855	Microsoft-Exchange Server
CVE-2021-26858	Microsoft-Exchange Server
CVE-2021-27065	Microsoft-Exchange Server
CVE-2021-26857	Microsoft-Exchange Server
CVE-2013-2551	Microsoft-Internet Explorer
CVE-2019-0752	Microsoft-Internet Explorer
CVE-2021-26411	Microsoft-Internet Explorer
CVE-2019-1367	Microsoft-Internet Explorer
CVE-2016-3351	Microsoft-Internet Explorer and Edge
CVE-2021-40444	Microsoft-MSHTML
CVE-2020-1472	Microsoft-Netlogon
CVE-2021-38646	Microsoft-Office
CVE-2017-11882	Microsoft-Office
CVE-2017-0199	Microsoft-Office and WordPad
CVE-2021-38647	Microsoft-Open Management Infrastructure (OMI)

CVE-2019-0604	Microsoft-SharePoint
CVE-2023-24955	Microsoft-SharePoint Server
CVE-2023-29357	Microsoft-SharePoint Server
CVE-2016-0034	Microsoft-Silverlight
CVE-2013-0074	Microsoft-Silverlight
CVE-2017-0145	Microsoft-SMBv1
CVE-2017-0144	Microsoft-SMBv1
CVE-2017-0147	Microsoft-SMBv1 server
CVE-2017-0148	Microsoft-SMBv1 server
CVE-2020-0796	Microsoft-SMBv3
CVE-2019-1069	Microsoft-Task Scheduler
CVE-2020-0638	Microsoft-Update Notification Manager
CVE-2018-8120	Microsoft-Win32k
CVE-2015-2546	Microsoft-Win32k
CVE-2015-1701	Microsoft-Win32k
CVE-2018-8453	Microsoft-Win32k
CVE-2019-1458	Microsoft-Win32k
CVE-2016-0167	Microsoft-Win32k
CVE-2021-1732	Microsoft-Win32k
CVE-2024-26169	Microsoft-Windows
CVE-2024-21338	Microsoft-Windows
CVE-2023-36884	Microsoft-Windows
CVE-2023-28252	Microsoft-Windows
CVE-2019-1388	Microsoft-Windows
CVE-2023-24880	Microsoft-Windows
CVE-2023-23376	Microsoft-Windows
CVE-2022-41073	Microsoft-Windows
CVE-2019-1385	Microsoft-Windows
CVE-2019-1130	Microsoft-Windows
CVE-2022-24521	Microsoft-Windows
CVE-2018-8440	Microsoft-Windows
CVE-2017-0213	Microsoft-Windows
CVE-2017-0146	Microsoft-Windows
CVE-2019-1405	Microsoft-Windows
CVE-2019-1322	Microsoft-Windows
CVE-2019-1315	Microsoft-Windows
CVE-2019-1253	Microsoft-Windows
CVE-2019-1129	Microsoft-Windows
CVE-2019-1064	Microsoft-Windows
CVE-2019-0841	Microsoft-Windows
CVE-2019-0543	Microsoft-Windows
CVE-2017-0101	Microsoft-Windows
CVE-2016-3309	Microsoft-Windows
CVE-2021-41379	Microsoft-Windows
CVE-2016-0099	Microsoft-Windows

CVE-2018-8174	Microsoft-Windows
CVE-2020-0787	Microsoft-Windows
CVE-2021-40449	Microsoft-Windows
CVE-2017-0143	Microsoft-Windows
CVE-2021-34527	Microsoft-Windows
CVE-2021-36942	Microsoft-Windows
CVE-2019-1215	Microsoft-Windows
CVE-2021-1675	Microsoft-Windows
CVE-2021-36955	Microsoft-Windows
CVE-2020-0609	Microsoft-Windows
CVE-2022-41223	Mitel-MiVoice Connect
CVE-2022-40765	Mitel-MiVoice Connect
CVE-2022-29499	Mitel-MiVoice Connect
CVE-2022-31199	Netwrix-Auditor
CVE-2022-21587	Oracle-E-Business Suite
CVE-2013-0431	Oracle-Java Runtime Environment (JRE)
CVE-2013-2465	Oracle-Java SE
CVE-2012-1723	Oracle-Java SE
CVE-2012-0507	Oracle-Java SE
CVE-2017-10271	Oracle-WebLogic Server
CVE-2019-2725	Oracle-WebLogic Server
CVE-2018-2894	Oracle-WebLogic Server
CVE-2020-2021	Palo Alto Networks-PAN-OS
CVE-2019-1579	Palo Alto Networks-PAN-OS
CVE-2023-27351	Papercut
CVE-2023-27350	PaperCut-MF/NG
CVE-2024-4577	PHP Group-PHP
CVE-2019-11043	PHP-FastCGI Process Manager (FPM)
CVE-2023-34362	Progress-MOVEit Transfer
CVE-2019-18935	Progress-Telerik UI for ASP.NET AJAX
CVE-2024-6670	Progress-WhatsUp Gold
CVE-2023-40044	Progress-WS_FTP Server
CVE-2023-48365	Qlik-Sense
CVE-2023-41266	Qlik-Sense
CVE-2023-41265	Qlik-Sense
CVE-2020-36195	QNAP-NAS
CVE-2018-19953	QNAP-Network Attached Storage (NAS)
CVE-2018-19949	QNAP-Network Attached Storage (NAS)
CVE-2018-19943	QNAP-Network Attached Storage (NAS)
CVE-2021-28799	QNAP-Network Attached Storage (NAS)
CVE-2022-27593	QNAP-Photo Station
CVE-2019-7195	QNAP-Photo Station
CVE-2019-7194	QNAP-Photo Station
CVE-2019-7192	QNAP-Photo Station
CVE-2019-7193	QNAP-QTS

CVE-2018-11138	Quest-KACE System Management Appliance
CVE-2023-38831	RARLAB-WinRAR
CVE-2018-20250	RARLAB-WinRAR
CVE-2010-1428	Red Hat-JBoss
CVE-2010-0738	Red Hat-JBoss
CVE-2017-12149	Red Hat-JBoss Application Server
CVE-2017-7494	Samba-Samba
CVE-2018-2380	SAP-Customer Relationship Management (CRM)
CVE-2021-42237	Sitecore-XP
CVE-2021-35211	SolarWinds-Serv-U
CVE-2020-5135	SonicWall
CVE-2019-7481	SonicWall
CVE-2021-20028	SonicWall-Secure Remote Access (SRA)
CVE-2021-20038	SonicWall-SMA 100 Appliances
CVE-2019-7481	SonicWall-SMA100
CVE-2024-40766	SonicWall-SonicOS
CVE-2021-20021	SonicWall-SonicWall Email Security
CVE-2021-20022	SonicWall-SonicWall Email Security
CVE-2021-20023	SonicWall-SonicWall Email Security
CVE-2021-20016	SonicWall-SSLVPN SMA100
CVE-2020-12271	Sophos-SFOS
CVE-2022-24682	Synacor-Zimbra Collaborate Suite (ZCS)
CVE-2018-6882	Synacor-Zimbra Collaboration Suite (ZCS)
CVE-2023-47246	SysAid-SysAid Server
CVE-2017-11357	Telerik-User Interface (UI) for ASP.NET AJAX
CVE-2022-24990	TerraMaster-TerraMaster OS
CVE-2024-40711	Veeam-Backup & Replication
CVE-2023-27532	Veeam-Backup & Replication
CVE-2022-26500	Veeam-Backup & Replication
CVE-2022-26501	Veeam-Backup & Replication
CVE-2021-27876	Veritas-Backup Exec Agent
CVE-2021-27877	Veritas-Backup Exec Agent
CVE-2021-27878	Veritas-Backup Exec Agent
CVE-2018-1273	VMware Tanzu-Spring Data Commons
CVE-2024-37085	VMware-ESXi
CVE-2020-3992	VMware-ESXi
CVE-2021-21974	Vmware-ESXI
CVE-2021-22005	VMware-vCenter Server
CVE-2021-21972	VMware-vCenter Server
CVE-2021-21985	VMware-vCenter Server
CVE-2019-5544	VMware-VMware ESXi and Horizon DaaS
CVE-2021-21975	VMware-vRealize Operations Manager API
CVE-2022-22954	VMware-Workspace ONE Access and Identity Manager
CVE-2022-29464	WSO2-Multiple Products
CVE-2022-41352	Zimbra Collaboration

CVE-2022-36537	ZK Framework-AuUploader
CVE-2022-47966	Zoho-ManageEngine
CVE-2021-40539	Zoho-ManageEngine
CVE-2024-11667	Zyxel-Multiple Firewalls

Reference:

- https://www.cert-in.org.in/s2cMainServlet?pageid=VLNLIST
- https://www.cert-in.org.in/s2cMainServlet?pageid=PUBADVLIST
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- https://www.cve.org

Ransomware Prevention & Mitigation Resources:

- https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES02&VLCODE=CIAD-2022-0023
- https://www.cert-in.org.in/s2cMainServlet?pageid=PUBWEL02
- https://www.csk.gov.in/documents/IndiaRansomwareReport2022.pdf
- https://www.csk.gov.in/documents/RANSOMWARE_Report_Final.pdf
- https://www.csk.gov.in/alerts/ransomware.html

****

Contact CERT-In For Any Technical Assistance

E-mail: incident@cert-in.org.in
Phone: +91-11- 22902657
Web: https://www.cert-in.org.in