NEWSLETTER

July 2024

National Critical Information Infrastructure Protection Centre

(A unit of National Technical Research Organisation)

VOLUME 8 ISSUE 3

@NCIIPC

NCIIPC Newsletter

July 2024

Inside This Issue

Message from the NCIIPC Desk

Dear Readers,

NCIIPC is committed to work with its stakeholders, national regulators, international partners and private organisations to protect Critical Information Infrastructure (CII) against cyber threats. Further NCIIPC has been developing strategies for planning, implementing and continually improving the technology-driven capabilities, processes and workforce for CII Protection (CIIP). In this newsletter we have tried to cover matters related to CIIP in India and across the globe during the second quarter of 2024.

NCIIPC's Responsible Vulnerability Disclosure Program provided opportunity for researchers to disclose vulnerabilities observed in Nation's Critical Information Infrastructure. There were 1913 vulnerabilities reported during the second quarter of 2024. Around 443 security researchers participated in RVDP programme in the second quarter of 2024.

A number of cyber security related initiatives have been witnessed in India and globally during the last quarter. Securities and Exchange Board of India (SEBI) has mandated that SEBI-regulated entities must adopt a Cybersecurity and Cyber Resilience Framework by specific deadlines in 2025. MeitY has lauched Cyber Surakshit Bharat initiative that aims to combat cybercrime by empowering Chief Information Security Officers (CISOs) and frontline IT officials. The Ministry of Home Affairs has planned to establish the Cyber Fraud Mitigation Centre, aimed at combatting cyber fraud in real-time to prevent financial losses for victims.

The White House released National Security Memorandum-22 to secure and enhance the resilience of U.S. Critical Infrastructure. NIST has published a public draft Product Development Cybersecurity Handbook, focused to secure Internet of Things. The seven prominent open-source foundations have collaborated to develop unified specifications and standards in anticipation of Europe's Cyber Resilience Act.

NCIIPC endevour is to involve with all stakeholders and take all necessary steps in safe, secure and resilient CII of nation.

Suggestions/Feedback from the readers are welcome. Please do write to us at newsletter@nciipc.gov.in. The important suggestions /feedback received shall also be published.

News Snippets - National

SEBI has Mandated SEBI-regulated Entities to Adopt the Cybersecurity and Cyber Resilience Framework

Securities and Exchange Board of India (SEBI) has mandated that SEBI-regulated entities must adopt a Cybersecurity and Cyber Resilience Framework (CSCRF) by specific deadlines in 2025. Entities regulated by SEBI must implement CSCRF based on their operational scale and specific thresholds in client base, trade volumes, and assets managed. The framework mandates compliance from six categories of entities by January 1, 2025, that already adhere to SEBI's cybersecurity guidelines. Other entities must adopt these standards by April 1, 2025. Key features include establishing Cyber Risk Governance, Data classification (Regulatory Data and IT/Cybersecurity Data), and deploying Security Operations Centre (SOC). It also outlines standards for API and mobile app security, introduces a Cyber Capability Index (CCI) for resilience assessment, and mandates Software Bill of Materials (SBOM) to mitigate supply chain risks. SEBI's initiative aims to fortify the cybersecurity posture of entities within its purview, ensuring robust protection against evolving cyber threats.

The framework mandates compliance from six categories of entities by January 1, 2025, that already adhere to SEBI's cybersecurity guidelines. Other entities must adopt these standards by April 1, 2025.

Cyber Surakshit Bharat Initiative by MeitY

In alignment with the 'Digital India' vision and amidst increasing cyber threats, the Ministry of Electronics and Information Technology (MeitY) launched the Cyber Surakshit Bharat initiative in collaboration with the National e-Governance Division (NeGD) and industry partners. The Cyber Surakshit Bharat initiative aims to combat cybercrime by empowering Chief Information Security Officers (CISOs) and frontline IT officials across government departments. It focuses on equipping them with the necessary capabilities to protect digital infrastructures from cyber-attacks. Key objectives include raising awareness, building capacities, and fostering a resilient cyber ecosystem within government entities. By promoting cyber safety and security, the initiative supports the efficient delivery of government services under the Digital India programme, ensuring robust protection of digital assets and citizen data.

The Cyber Surakshit Bharat initiative aims to combat cybercrime by empowering Chief Information Security Officers (CISOs) and frontline IT officials across government departments.

Global IndiaAI Summit 2024

The Government of India hosted the 'Global IndiaAI Summit' on 3-4 July 2024, in New Delhi delegates from 50 countries attended the summit. It featured 12 side sessions, which were graced by 2,000 global AI experts, Policy makers, Artificial Intelligence (AI)

Please refer page 24 & 25 for reference.

practitioners, Industry/Startups, and Academia. Over 10,000 AI enthusiasts joined the session virtually. The sessions focused on the fundamental aspects of the INDIAai Mission, showcasing India's proactive steps and dedication to establishing a comprehensive and equitable AI ecosystem domestically while aiming to spearhead global AI innovation.

Tackling Mobile Frauds in New Government's 100-day Plan

This service will inform call receivers about the identity linked to the SIM card used by the caller, enhancing transparency and security in telecommunications.

The Telecom Regulatory Authority of India (Trai) has recommended the Calling Name Presentation (CNAP) as a measure to curb fraud calls. The Calling Name Presentation service is expected to be operational within 100 days of the new government assuming office. This service will inform call receivers about the identity linked to the SIM card used by the caller, enhancing transparency and security in telecommunications. The telecom service provider will verify the identity of a caller and ensure that the accurate information is conveyed to the receiver. This initiative reflects the government's commitment to enhancing cybersecurity measures and protecting citizens' financial interests in an increasingly digital landscape.

RBI's Supervisory Action Against Indian Bank

The Reserve Bank of India (RBI) has directed one of the Indian Bank to halt the onboarding of new customers through its online and mobile banking platforms and to suspend the issuance of fresh credit cards due to significant concerns regarding the bank's IT infrastructure.

The Reserve Bank of India (RBI) has directed one of the Indian Bank to halt the onboarding of new customers through its online and mobile banking platforms and to suspend the issuance of fresh credit cards due to significant concerns regarding the bank's IT infrastructure. These concerns stem from examinations conducted by the RBI in 2022 and 2023, which revealed substantial deficiencies in various aspects of IT management, including inventory control, patch management, user access, vendor risk, data security, and business continuity in one of the Indian bank. Despite previous warnings and corrective measures, the bank's non-compliance persisted, resulting in frequent service disruptions, including a recent incident on April 15, 2024. In response, the RBI has imposed these restrictions to protect customers and mitigate the risk of prolonged service outages. The regulator in banking system is continuously giving such direction and emphasises the necessity for the bank. To address deficiencies comprehensively through an external audit, subject to RBI approval, to restore operational resilience and ensure the stability of the financial system.

Please refer page 24 & 25 for reference.

News Snippets - International

NIST Product Development Cybersecurity Handbook for IoT

NIST has published an initial public draft of its Product Development Cybersecurity Handbook, focusing on secure Internet of Things (IoT) products. This comprehensive guide addresses essential considerations for the development and deployment of IoT devices across diverse sectors and applications. The handbook expands NIST's existing efforts by emphasising cybersecurity beyond the IoT device itself to encompass all components involved in IoT product ecosystems. It highlights the potential risks introduced by vulnerable components, which often have privileged access to IoT devices and associated data, even if the primary device is secure.

This comprehensive guide addresses essential considerations for the development and deployment of IoT devices across diverse sectors and applications.

Open Source Foundations Unite on Common Standards for EU's Cyber Resilience Act

Seven prominent open-source foundations collaborated to develop unified specifications and standards in anticipation of Europe's Cyber Resilience Act (CRA), which was adopted by the European Parliament. The Apache Software Foundation, Blender Foundation, Eclipse Foundation, OpenSSL Software Foundation, PHP Foundation, Python Software Foundation, and Rust Foundation joined forces to consolidate their expertise and ensure alignment with the impending legislation. The CRA, introduced in draft form approximately two years ago, aimed to establish robust cybersecurity measures for internet-connected products sold within the European Union. It mandated manufacturers to maintain up-to-date patches and security updates, with penalties imposed for noncompliance. These penalties included fines scaling up to €15 million or 2.5% of global turnover. By pooling resources and integrating existing security best practices from open-source software development, the foundations aimed to fortify the software supply chain and enhance resilience against cyber threats as mandated by the CRA.

The CRA, introduced in draft form approximately two years ago, aimed to establish robust cybersecurity measures for internet-connected products sold within the European Union.

CISA Launched High-Risk Communities Webpage

CISA introduced a new High-Risk Communities webpage, offering essential cybersecurity resources tailored for civil society organisations facing elevated digital security threats. This webpage includes Project Upskill, which provides straightforward cyber hygiene guides, a repository of national cyber volunteer programs and access to a variety of free or heavily discounted cybersecurity tools and services.

Please refer page 24 & 25 for reference.

Analysis: Recognising that many civil society groups operate with limited budgets and are vulnerable to sophisticated cyber threats, CISA's initiative aims to bridge this gap with practical, accessible support.

NCSC Released New Version of Cyber Assessment Framework

The UK's National Cyber Security Centre (NCSC) has launched an updated version of its Cyber Assessment Framework (CAF), aimed at providing a structured approach to evaluating how organisations manage cyber risks to essential functions.

The UK's National Cyber Security Centre (NCSC) has launched an updated version of its Cyber Assessment Framework (CAF), aimed at providing a structured approach to evaluating how organisations manage cyber risks to essential functions. This new iteration of CAF, Cyber Assessment Framework V3.2, comes in response to analyses of global attacks on critical national infrastructure, prompting significant revisions in policies related to remote access, privileged operations, user access levels, and multi-factor authentication. The updated framework also incorporates alignment with cyber essentials requirements, a government-backed initiative designed to safeguard organisations against prevalent cyber threats. Notably, the latest version of CAF reflects the increasing influence of artificial intelligence, particularly in sections addressing automated functions and decision-making technologies.

White House Released National Security Memorandum-22

NSM-22 introduces a revised risk management cycle mandating Sector Risk Management Authorities (SRMAs) to identify, assess, and prioritize risks specific to their sectors.

On April 30, 2024, the National Security Memorandum (NSM)-22 on Critical Infrastructure Security and Resilience was issued by White House, outlining pivotal measures to fortify the security of vital sectors within the United States.

- NSM-22 introduces a revised risk management cycle mandating Sector Risk Management Authorities (SRMAs) to identify, assess, and prioritize risks specific to their sector.
- It emphasises the development of sector-specific risk management plans aimed at mitigating identified risks effectively.
- Emphasising collaboration between federal, state, local, tribal, and territorial entities, along with private sector stakeholders.
- The memorandum aims to enhance risk management capabilities and facilitate proactive defence strategies.

Key components include fostering robust information sharing frameworks to swiftly address emerging threats, including cyber vulnerabilities and physical disruptions. The memorandum stresses the integration of advanced technologies and best practices across critical infrastructure sectors, ensuring comprehensive protection against evolving challenges.

Please refer page 24 & 25 for reference.

Analysis: By promoting adaptive governance frameworks and coordinated response protocols, the memorandum seeks to mitigate potential impacts on infrastructure operations and public safety.

MITRE Systems Breached

MITRE, a non-profit organisation managing R&D centers disclosed details of a cyberattack on its unclassified Networked Experimentation, Research, and Virtualisation Environment (NERVE). The breach, first detected on December 31, 2023, involved a cyberespionage group from nation-state, which exploited two zero-day vulnerabilities (CVE-2024-46805 & CVE-2024-21887) in Ivanti secure VPN products. On January 4, 2024, the hackers started profiling the environment, interacting with VMware vCenter and ESXi hosts. The adversary started manipulating virtual machines and established control over the compromised infrastructure. MITRE only detected the intrusion in April. Between mid-February and mid-March, the hackers maintained persistence in the NERVE environment and attempted lateral movement, but did not succeed in accessing other resources.

The adversary started manipulating virtual machines and established control over the compromised infrastructure.

Analysis: The perimeter security devices are key elements to protect hence to be kept updated for protection from zero days, frequent reviews of network elements for any abnormality is SOC priority.

SCAA Suffered Cyberattack

The South China Athletic Association (SCAA) experienced a cyberattack on March 17, 2024, compromising member data such as names, birthdates, ID numbers, and addresses. In response, SCAA swiftly shut down the affected systems and reported the incident to law enforcement and the Office of the Privacy Commissioner for Personal Data (PCPD) in Hong Kong. The PCPD estimated that around 70,000 individuals were affected and had begun an investigation, urging SCAA to notify those impacted promptly. The potential victims were advised to change passwords, enable multi-factor authentication, monitor bank statements for unauthorised transactions, and be cautious of suspicious communications. They have also recommended vigilance against phishing attempts and scams. Members are advised to remain vigilant against potential misuse of their leaked information.

The PCPD estimated that around 70,000 individuals were affected and had begun an investigation, urging SCAA to notify those impacted promptly.

Please refer page 24 & 25 for reference.

Policy & Strategy

Strategy for CII Protection

In India, towards protection of the CII in sectors, both national agencies and sectoral regulator are issuing policies, procedures, guidelines and frameworks. Further, the regulatory guidelines define requirement of compliance to industry standards such as PCI-DSS, ISO 27001 etc. However, to mitigate the emerging threats strategies for CII Protections may include Risk Assessment at Sectoral Levels & at National level; improving robustness of implemented cyber security controls; and increasing resiliency across all critical sectors. Further, in order to do all these, working together with the industries and partner countries and also develop an ecosystem in the educational institutes or academia to provide adequate manpower technically skilled in CIIP specific technologies is advocated.

NCIIPC has been developing strategies for planning, implementing and continually improving the technology-driven capabilities, processes and workforce for CIIP.

One of the important functions of NCIIPC is to evolve strategy for protection of CII. NCIIPC has been developing strategies for planning, implementing and continually improving the technology-driven capabilities, processes and workforce for CIIP. Strategic like frameworks, tools and services can be developed as suggested in subsequent paragraphs:

- Cybersecurity Reference Framework at National Level: The Cybersecurity Reference Framework may brought out to provide critical sector and regulated entities in particular, and other organisations in general, a set of guidance to help them address their cyber security concerns in a systemic and structured manner.
- Cybersecurity Maturity Model (CMM): CMM may provide individual Critical Sector Entities (CSEs), and also enable national bodies like NCIIPC to carry out data-driven analytics from sectoral, cross-sectoral, and trends-over-time perspectives for strategical planning for CIIP.
- Collect, monitor and analyse logs/ feeds from Critical Information Infrastructure (CII) for situational awareness, threat forecasting and efficient incident response. This help in conducting statistical analysis and plan or improve the strategies for CIIP.
- Information Sharing Framework: Automated CII dissemination platform to collect threat intelligence from multiple sources and analyse the data, correlate the threat TTP/IOC in critical sectors and issue threat alerts on successful match. This will help in conducting statistical analysis and plan or improve the strategies for CIIP.
- Strategy to quickly identify and prioritise cyber security threats and risks to CII and roll out the mitigation strategies for example, during and post COVID-19, the concept of work from home has become popular in IT industry supporting CIIs. However, in parallel, this also opens a new set of attack

CMM may provide individual Critical Sector Entities (CSEs), and also enable national bodies like NCIIPC to carry out data-driven analytics from sectoral, cross-sectoral, and trends-over-time perspectives for strategical planning for CIIP.

*Please refer page 24 & 25 for reference.

surface, coming through the VPN connections of the employees working from home.

- How quickly can we detect such trends and more importantly, how quickly we can roll out threat mitigation strategies?

Improving Strategy for Cyber Resilience: Individual organisations may have their Business Continuity Plan (BCP), crisis or contingency and incident management plans. Further,

- Organisations to voluntarily share cyber security incidents
- Promulgating quantitative risk assessment mythologies for practical and accurate impact analysis for strategic decisions
- Conducting cyber security drills/ exercises involving multiple dependent sectors and requiring international cooperation

Promulgating quantitative risk assessment mythologies for practical and accurate impact analysis for strategic decisions

Public-Private-Partnership: The most mature CII organization is managed by the industry. To protect CII, active partnership with industry or private sector is required. PPP can help in filling the gaps in CIIP measures being taken up by the government agencies.

Secure-by-design products: To ensure that the CII applications are secure-by-design, security be incorporated in all the phases of SDLC. This includes following secure coding practices, risk assessments and static & dynamic security testing during the development of the software/applications.

To ensure that the CII applications are secure-by-design, security be incorporated in all the phases of SDLC.

Operational Technologies (ICS/SCADA/DCS): OT systems are inherently different than the IT systems, and have their unique security challenges. Cyber security strategies focused on data-security strategy may not be applied to OT systems, as these are more focused on availability aspects. However, both IT and OT systems are now converging. Strategy for secure IT-OT convergence has to be developed with due considerations on business requirements.

Malware Bytes

Metasploit Meterpreter Installed via Redis Server

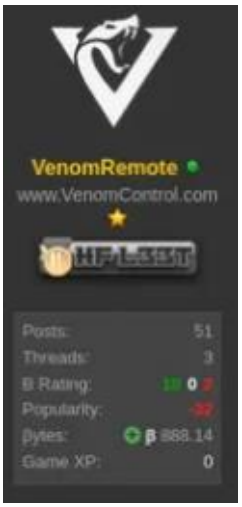
A significant security issue involving the installation of the Metasploit Meterpreter backdoor via externally exposed Redis (Remote Dictionary Server) servers was reported. Specifically targeting Redis versions dating back to 2016, the vulnerabilities that were adequately managed are susceptible to exploitation. Metasploit is a framework used for penetration testing. It helps identify security vulnerabilities in networks and systems of organisations by offering a range of tools tailored to each stage of the testing process. Once installed, Metasploit Meterpreter grants threat actors full control over compromised systems, potentially extending their reach to internal networks. To mitigate these risks, security managers are urged to promptly patch Redis

Once installed, Metasploit Meterpreter grants threat actors full control over compromised systems, potentially extending their reach to internal networks.

*Please refer page 24 & 25 for reference.

servers to the latest versions and adopt stringent access controls for externally open servers. Additionally, deploying protective software is recommended to fortify defenses against unauthorised access attempts.

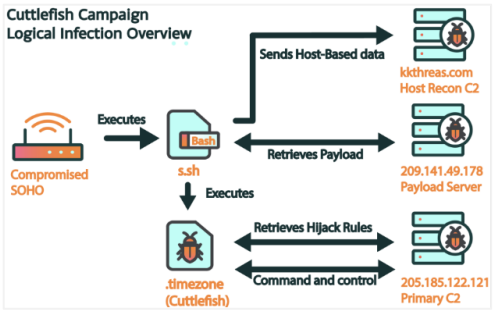
Venom RAT Targeted Multiple Sectors



VenomRAT introduction on malware-oriented forums

TA558, a known threat actor, launched an extensive phishing campaign targeting various sectors across Latin America, aiming to deploy Venom RAT. The campaign specifically targeted industries including hospitality, travel, finance, manufacturing, government, and others in multiple countries. Venom RAT, derived from Quasar RAT, possesses sophisticated capabilities for data harvesting and remote system control. The attack begins with phishing emails designed to serve as the initial point of entry. These emails deliver Venom RAT, which enables attackers to access compromised systems. This access allows them to conduct a range of malicious activities, posing a significant threat to affected organisations. Researchers from Perception Point have identified this latest infection chain, emphasising the strategic use of phishing tactics to distribute Venom RAT. To mitigate the risk posed by TA558's operations, organisations in the targeted sectors must prioritise vigilant monitoring and proactive security measures.

Cuttlefish Malware Infects Routers



Cuttlefish infection chain (Source: Black Lotus Labs)

A newly identified malware called 'Cuttlefish' has targeted both enterprise-grade and Small Office/Home Office (SOHO) routers, with the aim of intercepting data passing through these devices to steal authentication information. To achieve this, Cuttlefish installs a proxy or VPN tunnel on compromised routers, enabling discreet exfiltration of data while circumventing security systems designed to detect unusual logins. Additionally, the malware can execute DNS and HTTP hijacking within local IP networks, potentially introducing further malicious payloads and disrupting internal communications. Once it gains access to a router, Cuttlefish deploys a bash script ("s.sh") to gather host-based data such as directory listings, running processes, and active connections. It then downloads and executes its primary payload (".timezone") into memory, erasing the file from the system to avoid detection. The malware utilises a packet filter to passively monitor all connections through the device, scanning for specific data termed "credential markers" (e.g., usernames, passwords, tokens), particularly those linked to cloud-based services. Cuttlefish takes action based on regularly updated rulesets received from the attacker's Command and Control (C2) server upon detecting such data.

Cuttlefish takes action based on regularly updated rulesets received from the attacker's Command and Control (C2) server upon detecting such data.

Please refer page 24 & 25 for reference.

Agenda Ransomware Propagates via Custom PowerShell Script

An updated version of the Agenda ransomware has intensified its threat landscape by leveraging a custom PowerShell script to propagate through VMware vCenters and ESXi servers. This sophisticated tactic exploits vulnerabilities in VMware's infrastructure, enabling Agenda to infiltrate and encrypt Virtual Machines (VMs) and their associated data, facilitating unauthorised access and deployment of malicious payloads. Agenda swiftly encrypts critical files and demands ransoms for decryption keys, causing severe disruptions and losses for affected organisations.

Advisory: Organisations utilising VMware technologies must remain vigilant, implement stringent access controls, regular security updates, and proactive threat detection mechanisms to thwart Agenda's propagation attempts and mitigate the risk of ransomware attacks.

An updated version of the Agenda ransomwar has intensified its threat landscape by leveraging a custom PowerShell script to propagate through VMware vCenters and ESXi servers.

MuddyWater Hackers Adopt New C2 Tool 'DarkBeatC2'

MuddyWater threat actor group has unveiled a new Command-and-Control (C2) infrastructure dubbed DarkBeatC2. Their latest campaign initiated with targeted spear-phishing emails originating from compromised accounts. These emails contain links or attachments hosted on platforms such as Egnyte, facilitating the delivery of the Atera Agent software. Once initiated, the attack focuses on establishing persistence within the compromised system.

The threat actor achieves this by creating a scheduled task that triggers PowerShell scripts leveraging the AutodialDLL registry key to load the necessary DLL for their C2 framework. Alternatively, they utilise DLL side-loading techniques, exploiting legitimate applications to execute malicious code undetected. Successful contact with the C2 server enables the infected host to receive and execute PowerShell scripts. These PowerShell scripts serve various purposes, including fetching additional payloads and transmitting gathered data, such as the contents of 'C:\ProgramData\SysInt.log', via HTTP POST requests. Another script periodically polls the server for new instructions and logs execution results to 'SysInt.log'. The threat actors are updating their TTPs to bypass traditional security tools.

Once initiated, the attack focuses on establishing persistence within the compromised system. MuddyWater achieves this by creating a scheduled task that triggers PowerShell scripts leveraging the AutodialDLL registry key to load the necessary DLL for their C2 framework.

ArcaneDoor - New Espionage-focused Campaign

A global cyber-espionage operation, dubbed 'ArcaneDoor,' was initiated by an unknown threat actor UAT4356, leveraging two undisclosed vulnerabilities in Cisco firewall devices to breach government network perimeters. This sophisticated attack chain involves the exploitation of these vulnerabilities to implant custom-built backdoors, namely "Line Dancer" and "Line Runner," on targeted Cisco Adaptive Security Appliance (ASA) devices. Once

Please refer page 24 & 25 for reference.

Once compromised, UAT4356 employs these backdoors to execute malicious commands and implant malware across a select group of CISCO customers.

compromised, UAT4356 employs these backdoors to execute malicious commands and implant malware across a select group of CISCO customers. The Line Dancer backdoor facilitates the submission of shellcode through the host-scan-reply field, enabling the attackers to execute commands. To maintain persistence, UAT4356 utilises the Line Runner backdoor, exploiting legacy functionality associated with pre-loading VPN clients and plugins on compromised ASA devices.

Large-Scale StrelaStealer Campaign

StrelaStealer spreads primarily through spear phishing emails containing ZIP file attachments.

Palo Alto Networks researchers have identified a significant surge in StrelaStealer malware campaigns impacting over 100 organisations in both the EU and U.S. These campaigns involve spam emails carrying attachments that initiate the execution of StrelaStealer's DLL payload. StrelaStealer spreads primarily through spear phishing emails containing ZIP file attachments. Upon opening the archive, a JScript file is deposited onto the system, followed by the placement of a Base64-encrypted file and a batch file. Using the certutil -f decode command, the Base64-encrypted file is decoded, generating a Portable Executable (PE) DLL file. Depending on the user's privileges, this file is dropped into either "%appdata%\temp" or "c:\temp" on the local disk. Subsequently, the DLL file is executed via the exported function "hello" using rundll32.exe.

Learning

Attack Surface Management vs. Vulnerability Management

Alert & Advisory Team, NCIIPC

In the ever-evolving landscape of cybersecurity, organisations adopt advanced strategies like Attack Surface Management (ASM) and Vulnerability Management (VM) to protect their digital assets. Though similar, these methods target different cybersecurity aspects, and their integration shall significantly enhance organisation's security.

ASM is a proactive strategy focusing on identifying, monitoring, and reducing risks associated with an organisation's digital presence.

Attack Surface Management (ASM): ASM is a proactive strategy focusing on identifying, monitoring, and reducing risks associated with an organisation's digital presence. It includes both known and unknown assets that attackers might exploit, providing a comprehensive view of the attack surface from an adversary's perspective. The key components of ASM are as follows:

- Discovery: Continuous scanning and mapping of digital assets to uncover potential entry points.
- Assessment: Evaluating identified assets for vulnerabilities and security weaknesses.
- Prioritisation: Ranking assets based on criticality and potential impact.
- Remediation: Mitigating identified risks through actions like patching vulnerabilities.

Please refer page 24 & 25 for reference.

- Monitoring: Ongoing surveillance to detect new assets and emerging threats in real-time.

Vulnerability Management (VM): VM is a traditional cybersecurity approach focusing on identifying, assessing, and mitigating vulnerabilities in known assets. Its goal is to reduce exploitation risks by promptly addressing vulnerabilities. The key components of VM are as follows:

VM is a traditional cybersecurity approach focusing on identifying, assessing, and mitigating vulnerabilities in known assets.

- Identification: Using automated tools to scan systems, networks, and applications for known vulnerabilities.
- Evaluation: Assessing the severity and potential impact of identified vulnerabilities.
- Prioritisation: Ranking vulnerabilities based on risk level to address critical threats first.
- Remediation: Applying patches or other measures to fix vulnerabilities.
- Verification: Rescanning assets post-remediation to ensure vulnerabilities are resolved.

Key Differences between ASM and VM:

- Scope:
  ASM: Encompasses the entire digital footprint, including unknown assets.
  VM: Focuses on known assets.
- Perspective:
  ASM: Adopts an external attacker's viewpoint.
  VM: Operates from an internal perspective.
- Approach:
  ASM: Proactive and continuous.
  VM: Reactive and periodic.
- Tools and Techniques:
  ASM: Uses advanced discovery tools and continuous monitoring.
  VM: Relies on automated scanning tools and vulnerability databases.

Combining ASM and VM provides a comprehensive cybersecurity strategy addressing both known and unknown risks.

Integrating ASM and VM: Combining ASM and VM provides a comprehensive cybersecurity strategy addressing both known and unknown risks.

- Holistic View: Covers all assets and vulnerabilities.
- Enhanced Prioritisation: Improves remediation focus.
- Improved Efficiency: Streamlines risk identification and mitigation.
- Continuous Improvement: Maintains ongoing awareness and quick threat response.

Due to complexity of cloud ecosystems, irrespective of private on-prem deployment or public cloud deployment, most of the Critical Sector Entities (CSEs) depend on MSP and MSSPs to manage their services.

To effectively combat evolving cyber threats, integrating Attack Surface Management (ASM) and Vulnerability Management (VM) is essential. ASM offers a proactive view of potential risks, while VM focuses on known vulnerabilities. Together, they provide a

Please refer page 24 & 25 for reference.

comprehensive, resilient security strategy, protecting digital assets from diverse threats.

Managed Service Provider & Managed Security Service Provider

A third-party entity known as a Managed Service Provider (MSP) oversees and handles a customer's IT framework and/or user-facing systems, often operating proactively and offering services through a subscription-based approach. MSPs provide a range of services including network, application, infrastructure, and security management. These services are delivered through ongoing assistance and direct management either on-site at the client's location, within the MSP's own data centre (hosting), or at a data centre owned by another party.

DPDP Act not only directs the data processors to apply reasonable security safeguards to prevent personal data breaches, but also speaks about imposing penalty, in the event of a personal data breach due to the absence of a required remedial or mitigation measures.

On the other hand, a Managed Security Service Provider (MSSP) is a specialised type of MSP that focuses solely on security services. An MSSP offers external management and surveillance of security mechanisms and systems. Due to complexity of cloud ecosystems, irrespective of private on-prem deployment or public cloud deployment, most of the Critical Sector Entities (CSEs) depend on MSP and MSSPs to manage their services. CSEs are actively seeking the benefits of transitioning their technology platforms and services to the cloud by utilising one or more of the primary cloud service models – Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). However, subscriptions to these services often entail security and compliance challenges that they must be prepared to resolve.

Current Status: In India CSEs are encouraged to adopt Government Community Cloud (GCC) called- "GI Cloud" or "MeghRaj"; or alternatively subscribe to the GCC complaint Cloud services. Ministry of Electronics and Information Technology (MeitY) empanels GCC compliant Cloud Service Providers (CSPs). Most of the CSEs having Cloud usage take services of MSP and MSSPs to manage and secure their infrastructure.

India also has legal provisions which emphasis requirement of Cloud Security:

- Digital Personal Data Protection Act 2023 (DPDP Act): DPDP Act not only directs the data processors to apply reasonable security safeguards to prevent personal data breaches, but also speaks about imposing penalty, in the event of a personal data breach due to the absence of required remedial or mitigation measures.
- Security of CII hosted over Cloud is covered under the ambit of Section 70 of Information Technology Act, 2000 (IT Act),

While outsourcing IT security services can offer various benefits, it also comes with certain risks and challenges that CSEs need to consider and manage effectively.

While outsourcing IT security services can offer various benefits, it also comes with certain risks and challenges that critical sector

Please refer page 24 & 25 for reference.

need to consider and manage effectively. Some common risks associated with outsourcing IT security services are:

- Loss of Visibility & Control: Outsourcing IT management and information security may result in loss of visibility and control over security processes, policies, and operations. Organisations have to ensure that the service provider's practices align with their security requirements and standards.
    - Is the MSP properly segregating applications/data/infrastructure of multiple clients?
        - How does the MSP serve organisations with different security requirements / maturity levels?
        - What would be impact of breach of a shared back-end infrastructure?
- Incident Reporting: How to ensure that the MSPs/MSSPs are reporting the security incident properly, as this might cause a negative reputation value or a financial penalty.
- Is the Security Operation Centre is getting logs from all the sources?
- Is there provision of adequate and dedicated manpower?
- Confidentiality Concerns: Organisations have to establish safeguards to protect sensitive, confidential data.
    - How to ensure that the critical data is not directly accessible/ visible to the MSP?
- Supply Chain Risks: Organisations may be exposed to supply chain risks, including vulnerabilities in the service provider's infrastructure, subcontractors, or third-party vendors. Organisations have to conduct diligence and risk assessments throughout the supply chain.
- Dependency: Reliance on a single service provider for critical security functions can create a dependency risk. Organisations have to diversify their security measures and consider contingency plans in case of service disruptions or provider issues.
    - How to ensure secure "Exit Management plan": Offboarding

Organisations can seek these answers from MSP/MSSP before taking the services.

Reliance on a single service provider for critical security functions can create a dependency risk. Organisations have to diversify their security measures and consider contingency plans in case of service disruptions or provider issues.

Ransomware and Personal Data Protection in Healthcare

Advances in technology have helped the healthcare industry to replace paper-based systems with Electronic Health Records (EHR). EHRs enhance patient care, develop patient cooperation, enhance disease diagnosis, improve practice efficiency, and make patient health information accessible all the time. But unfortunately, every blessing has a curse, which also applies here. Due to software vulnerabilities, security failures, and human error, these databases are sometimes accessed by unauthorised users. This leads to exposure of sensitive data in form of data breaches. Ransomware attacks also represent a pervasive and escalating threat within the

EHRs enhance patient care, develop patient cooperation, enhance disease diagnosis, improve practice efficiency, and make patient health information accessible all the time.

Please refer page 24 & 25 for reference.

healthcare sector. Every year, the sophistication and frequency of these cyber-attacks continue to rise, wreaking havoc on institutions.

From 2005 to 2019, the total number of individuals affected by healthcare data breaches were 249.09 million. As per IBM, the average cost of a data breach in 2019 was $3.92 million, while a healthcare industry breach typically costs $6.45 million. Healthcare data is more sensitive than other types of data because any data tampering can lead to faulty treatment, with fatal and irreversible losses to patients.

The sharing of experience and effective strategies to deal in case an organisation has become victim of Ransomware attack or sensitive data breach.

Ransomware attacks result in disruptive downtime as healthcare providers are unable to access vital patient information. These interruptions to the flow of information lead to delays in medical procedures, appointment cancellations, and compromised patient care. The disabling of patient registration system leads to long physical queues and possible law & order chaos. Moreover, the attackers commonly demand hefty ransom payments in exchange for decryption keys, further exacerbating the financial burden on already strained budgets.

The entities in health sector shall work on the following to improve security posture against ransomware attacks.

- The security measures to prevent ransomware attacks and breach of Personal Health Information.
- The sharing of experience and effective strategies to deal in case an organisation has become victim of Ransomware attack or sensitive data breach.
- The legal and procedural directives to manage such issues and ensuring public trust on the system.
- The national and international collaborative mechanisms to handle such burning issues of healthcare security.

Role of AI/ML in Protection of CII

Cyber threats have evolved from simple viruses and malware to complex, multi-vector attacks that can cripple entire networks and services. These threats include Advanced Persistent Threats (APTs), ransomware, phishing attacks, and state-sponsored cyber espionage. The dynamic nature of these threats requires a defense mechanism that is equally dynamic and capable of learning and adapting in real-time. These technologies can analyse vast amounts of data, identify patterns, and detect anomalies that may indicate potential cyber threats. Here are some key areas where AI and ML are making a significant impact.

AI can help protection of CII by supporting threat detection & prevention, automating incident response, improving threat and vulnerability analytics, anomaly detection, natural language processing etc.

- AI can help protection of CII by supporting threat detection & prevention, automating incident response, improving threat and vulnerability analytics, anomaly detection, natural language processing etc.

Please refer page 24 & 25 for reference.

The modern CII is widespread and complex making it difficult to estimate and have control over the entire attack surface, especially with operational technology system like those in power systems, oil & gas pipelines, country-wide rail network etc.

AI in the modern day has potential applications in all sectors, therefore, collaborative development of AI/ML technologies while keeping security in mind right from the beginning is very important.

There is need of enhanced detection capabilities and better automation in response while maintaining critical balance with business continuity. Only cyber threats do not form the complete challenge, the utilisation of AI/ML technologies for competitive gains, efficient operations and predictive maintenance also exposes newer attack surface.

AI in the modern day has potential applications in all sectors, therefore, collaborative development of AI/ML technologies while keeping security in mind right from the beginning is very important.

Vulnerability Watch

Critical Vulnerability in Palo Alto Networks

A critical vulnerability, identified as CVE-2024-3400 having CVSS score 10.0, has been discovered in the GlobalProtect feature of Palo Alto Networks PAN-OS software. This vulnerability arised from an arbitrary file creation flaw, leading to command injection. On exploitation, it can allow an attacker without authentication to execute arbitrary code with root privileges on the affected firewall. The vulnerability, CVE-2024-3400, affects PAN-OS 10.2, PAN-OS 11.0, and PAN-OS 11.1 firewalls when configured with GlobalProtect gateway or GlobalProtect portal, or both. Users are recommended to upgrade to a patched version of PAN-OS to ensure the security of their devices, even if workarounds and mitigations have been implemented.

This vulnerability arised from an arbitrary file creation flaw, leading to command injection.

Critical Vulnerability in xz Libraries

A malicious code was discovered in the upstream tarballs of xz libraries, a general purpose data compression format present in almost every Linux distribution, beginning with version 5.6.0. This vulnerability has been assigned CVE ID CVE-2024-3094 having CVSS score 10.0. This code injection occured through a sophisticated process within the liblzma build system. The resulting liblzma library is modified, capable of intercepting and manipulating data interactions with any software linked against it. Fedora Rawhide and Fedora Linux 40 beta were affected by this vulnerability. It is recommended to all Fedora Linux 40 beta users to revert to 5.4.x versions and Fedora Rawhide to revert to xz-5.4.x.

This code injection occured through a sophisticated process within the liblzma build system. It involves extracting a prebuilt object file from a disguised test file within the source code.

Critical Vulnerability in CrushFTP

Critical server side template injection vulnerability in CrushFTP. CrushFTP is a robust file transfer server. This server side template

Please refer page 24 & 25 for reference.

All versions of CrushFTP before 10.7.1 and 11.1.0 have been affected by this vulnerability.

injection vulnerability has CVE ID CVE-2024-4040 having CVSS score 10.0. The affected firmware allows unauthenticated remote attackers to read files from the filesystem outside of the VFS Sandbox, bypass authentication to gain administrative access, and perform remote code execution on the server. All versions of CrushFTP before 10.7.1 and 11.1.0 have been affected by this vulnerability.

The attack operates by tricking VPN users into believing their connections are securely encrypted and routed through a protected tunnel, when in reality, the traffic is redirected to the attacker's server for potential inspection.

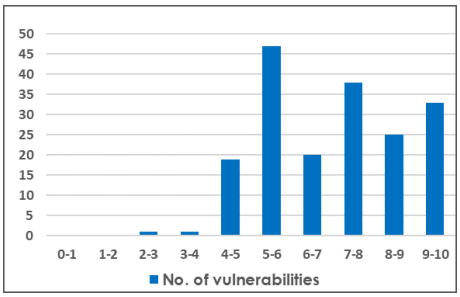
New TunnelVision Attack Allows Hijacking of VPN Traffic

TunnelVision, a newly exposed VPN bypass technique, poses a significant threat to network security by allowing attackers to intercept and manipulate VPN traffic with ease. TunnelVision attack has been assigned CVE-2024-3661 having CVSS score 7.6, this vulnerability affects all operating systems featuring a DHCP client and supporting DHCP option 121 routes. The attack operates by tricking VPN users into believing their connections are securely encrypted. To mitigate this risk, organisations are urged to implement robust defensive measures, including DHCP snooping, ARP protections, and port security on switches. Furthermore, deploying network namespaces on Linux systems is recommended to rectify the underlying behavior exploited by TunnelVision.

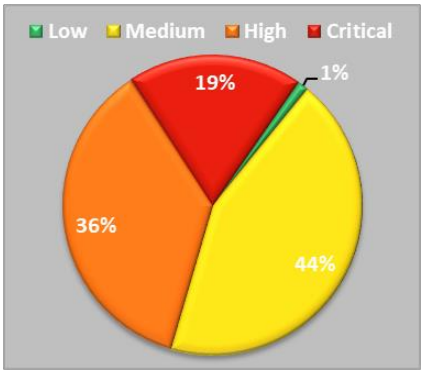
Quarterly Vulnerability Analysis Report

Alert & Advisory Team, NCIIPC

During the second quarter of 2024, a total of 184 vulnerabilities have been observed, out of which majority of vulnerabilities have score ranging from 4-7. 19 percent of total vulnerabilities reported were of critical severity. Linux, Tenda, Google, IBM, Apple and Microsoft were the top six vendors having 71% of total reported vulnerabilities.



Severity-wise number of vulnerabilities

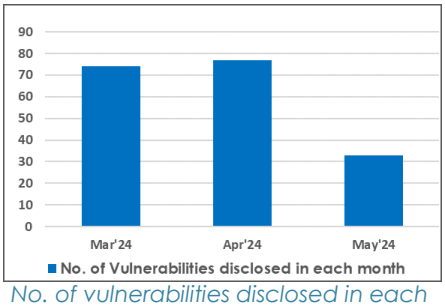


Severity-wise share of vulnerabilities

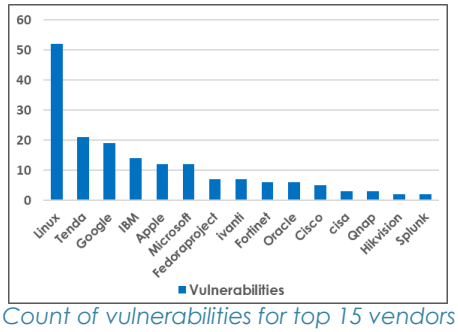
Severity	CVSSv 3 Score	Number of Vulnerabilities			Total Vulnerabilities	Severity Total
		Mar'24	Apr'24	May'24		
Low	0-1	0	0	0	0	02
	1-2	0	0	0	0	
	2-3	1	0	0	1	
	3-4	0	1	0	1	
Medium	4-5	15	4	0	19	86
	5-6	7	22	18	47	
	6-7	7	12	1	20	
High	7-8	9	22	7	38	63
	8-9	10	9	6	25	
Critical	9-10	25	7	1	33	33
Total		74	77	33		184

Please refer page 24 & 25 for reference.

S. No.	Vendor	No. of Vulnerabilities			Total
		Mar'24	Apr'24	May'24	
1.	Linux	0	29	23	52
2.	Tenda	19	2	0	21
3.	Google	7	9	3	19
4.	IBM	10	4	0	14
5.	Apple	12	0	0	12
6.	Microsoft	3	7	2	12
7.	Fedoraproject	7	0	0	7
8.	Ivanti	2	4	1	7
9.	Fortinet	6	0	0	6
10.	Oracle	0	6	0	6
11.	Cisco	0	4	1	5
12.	CISA	3	0	0	3
13.	Qnap	3	0	0	3
14.	Hikvision	2	0	0	2
15.	Splunk	2	0	0	2



No. of vulnerabilities disclosed in each month

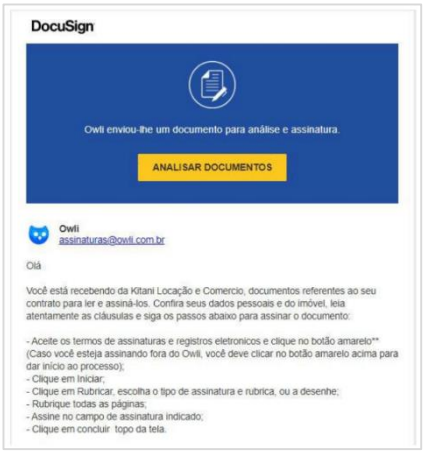


Count of vulnerabilities for top 15 vendors

Mobile Security

CHAVELOAK: The Latest Banking Trojan Threat Targeting Brazil

The cyber security landscape is constantly evolving, with new threats emerging regularly to exploit vulnerabilities and compromise sensitive data. A new banking Trojan dubbed "CHAVELOAK" has emerged that specifically targeted users in Brazil. CHAVELOAK represents a significant threat to individuals and organisations alike, with its sophisticated capabilities designed to steal financial information and carry out fraudulent transactions. This malicious software operates by infiltrating systems through malicious PDF attachments. CHAVELOAK discreetly monitors user activity, intercepting sensitive data such as login credentials, banking details, and personal information. What makes CHAVELOAK particularly alarming is its ability to evade detection by traditional antivirus software and security measures. This trojan employs advanced techniques to conceal its presence and resist removal, making it challenging for users to detect and mitigate the threat effectively.



The malicious PDF file

Microsoft Alerts Users to "Dirty Stream" Attack

In the ever-evolving landscape of cyber security threats, vigilance is key to safeguarding our digital assets. Today, your attention to a concerning development is sought: Microsoft's recent warning about the "Dirty Stream" attack, which poses a significant risk to Android app users. The "Dirty Stream" attack targets Android apps, exploiting vulnerabilities in Android's content provider system functionality. This attack vector allows malicious actors to inject and execute arbitrary code within the context of the targeted app, potentially leading to a range of harmful consequences, including

The "Dirty Stream" attack targets Android apps, exploiting vulnerabilities in Android's content provider system functionality.

Please refer page 24 & 25 for reference.

data theft, device compromise, and unauthorised access. Microsoft's Threat Intelligence Centre has identified this threat and is actively monitoring its evolution. While specific details about the attack methodology and affected apps remain limited, the potential impact is substantial, given the widespread use of Android devices and streaming apps.

Android 'eXotic Visit' Spyware

The 'eXotic Visit' spyware campaign is a newly identified cyber threat targeting Android users. The spyware is distributed through malicious apps masquerading as legitimate services, such as messaging apps or SIM information tools, both through dedicated websites and the Google Play Store. These malicious apps embed the XploitSPY Remote Access Trojan (RAT), which allows attackers to gain extensive access to the victim's device. Once installed, the spyware can steal sensitive information, including text messages, call logs, contact lists, and even location data. Additionally, it can capture screenshots, record audio, and take photos using the device's camera, making it a comprehensive tool for surveillance and data theft. One of the key tactics employed in this campaign involves exploiting users' trust in popular applications. The attackers create convincing replicas of well-known apps, tricking users into downloading the infected versions. Despite Google Play Store's security measures, some of these apps have managed to bypass defences and reach unsuspecting users.

Once installed, the spyware can steal sensitive information, including text messages, call logs, contact lists, and even location data.

The New Android Trojan SoumniBot Evade Detections

A new strain of Android banking malware, Soumnibot, has been identified, featuring sophisticated techniques to evade detection, according to Kaspersky. This malware primarily targets users in Korea and Brazil by obfuscating its app manifest to bypass traditional security measures. Soumnibot employs advanced obfuscation methods, making it difficult for security researchers to analyse and detect its malicious activities. The malware hides its intentions by scrambling critical information within the app manifest, a key component that describes the application's structure and permissions. This obfuscation allows Soumnibot to stealthily install itself on victims' devices without raising alarms. Once installed, Soumnibot gains access to sensitive information such as banking credentials, personal identification numbers, and other financial data. The malware is capable of intercepting and stealing SMS messages, which are often used for two-factor authentication (2FA) by banks, thereby compromising additional layers of security. Kaspersky's analysis highlights the importance of being vigilant when downloading apps, especially from unofficial sources. Users are advised to only download apps from trusted platforms like Google Play and to be cautious about granting permissions to apps that request access to sensitive information.

Soumnibot employs advanced obfuscation methods, making it difficult for security researchers to analyse and detect its malicious activities.

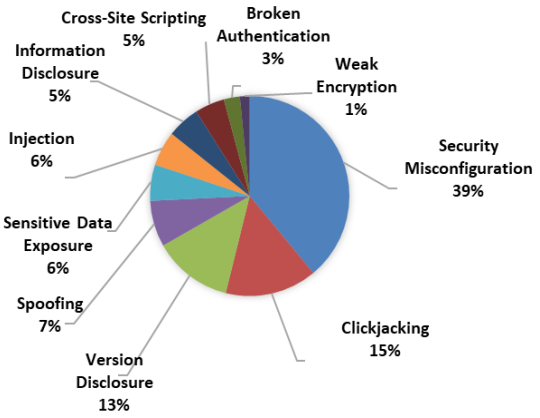
Please refer page 24 & 25 for reference.

NCIIPC Initiatives

NCIIPC Responsible Vulnerability Disclosure Program

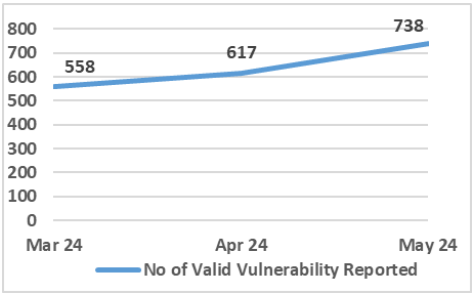
The NCIIPC Responsible Vulnerability Disclosure Program provides opportunity for researchers to disclose vulnerability observed in Nation's Critical Information Infrastructure. There are 1913 vulnerabilities reported during the second quarter of 2024. The top 10 vulnerabilities are:

- Security Misconfiguration
- Clickjacking
- Version Disclosure
- Spoofing
- Sensitive Data Exposure
- Injection
- Information Disclosure
- Cross-Site Scripting
- Broken Authentication
- Weak Encryption



Around 443 security researchers participated in RVDP programme during the second quarter of 2024. NCIIPC acknowledges following top 15 researchers for their contributions (names are in alphabetical order):

- Alan Sheri
- Azif Mhammed K
- Chinmay Chougule
- Chinmay Rana
- Gautam Rawat
- Harikrishnan K V
- Harshit Kumar
- Ishank Malviya
- K Shanmukhasrisai
- Kiran Scaria
- Pradip Dey
- Prishak Kumar
- Rizwan Syed
- Soorya Narayanan Au
- Srinivasan



Last three months' timeline chart for vulnerabilities reported

Please refer page 24 & 25 for reference.

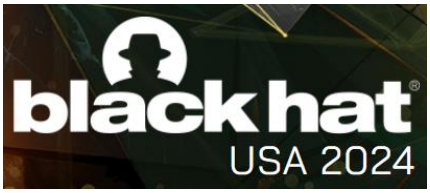
Events - Global

JULY 2024

S	M	T	W	T	F	S
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

AUGUST 2024

S	M	T	W	T	F	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31



July 2024

- PhilSec Cyber Security Summit 2024, Manila 2-3 Jul
- Strategy Summit Cyber Security, Berlin 3-4 Jul
- FinCrime & Cybersecurity Summit, Sydney 4 Jul
- Pittsburgh Cybersecurity Conference, Pittsburgh 11 Jul
- Phoenix-Scottsdale Cybersecurity Conference, Scottsdale 18 Jul
- IANS: CISO Roundtable National 2024, Virtual 24 Jul
- Gartner Data & Analytics Summit, Sydney 29-30 Jul
- INTERFACE Montana 2024, Montana 31 Jul

August 2024

- Minneapolis Cybersecurity Conference, Minneapolis 2 May
- Black Day 2024, Las Vegas 3-8 Aug
- BSides Las Vegas, Las Vegas 6-7 Aug
- Devopsdays Minneapolis, Minneapolis 6-7 Aug
- DEF CON 32, Las Vegas 8-11 Aug
- CISO Executive Network, Sydney 12 Aug
- Salt Lake City Cybersecurity Conference, Salt Lake City 15 Aug
- PAICTA Cybersecurity4D Conference, East London 21-23 Aug
- International Summit on Robotics and Artificial Intelligence, Valencia 26-28 Aug

September 2024

- INFOSEK, Nova Gorica 4-6 Sep
- FinCrime & Cybersecurity Summit, Frankfurt 5 Sep
- BSidesCache, Logan 6 Sep
- FranSec Cyber Summit, Paris 10-11 Sep
- GoSec 2024, Montreal 11-12 Sep
- CRESTCon Australia 2024, 26 Sep
- SecureWorld St. Louis, St. Louis 26 Sep
- NetDiligence: Cyber Risk Summit, Philadelphia 30 Sep-02 Oct

October 2024

- Cyber Security & Cloud Expo, Amsterdam 1-2 Oct
- CISO 360 Asia & Oceania Conference, Melbourne 2-3 Oct
- Innovate Cybersecurity Summit, Scottsdale 6-8 Oct
- SecureWorld New York City, New York City 15 Oct
- Governance 360 Africa, Mombasa 23-25 Oct
- Next IT Security Nordics, Stockholm 26 Oct
- Forum InCyber 2024, Montreal 29-30 Oct
- Devopsdays Tel Aviv, Tel Aviv 30-31 Oct

Events - India

- Global IndiaAI Summit, New Delhi 3-4 Jul
- Meridian Conference 2024, New Delhi 3-6 Jul
- Mirai 24, New Delhi 5 Jul
- BFSI IT Summit, Mumbai 1 Aug
- ESCON24, Haryana 23-25 Aug
- India Cloud Summit, New Delhi 29 Aug
- World CyberCon 2024, Mumbai 27 Sep
- India Cloud Summit, Hyderabad 23 Oct

SEPTEMBER 2024

S	M	T	W	T	F	S
30						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29

OCTOBER 2024

S	M	T	W	T	F	S
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

General Help	helpdesk1@nciipc.gov.in helpdesk2@nciipc.gov.in
Incident Reporting	: ir@nciipc.gov.in
Vulnerability Disclosure	: rvdp@nciipc.gov.in
Malware Upload	: mal.repository@nciipc.gov.in

Abbreviations

- APT: Advanced Persistent Threat
- ASM: Attack Surface Management
- BCP: Business Continuity Plan
- CAF: Cyber Assessment Framework
- CCI: Cyber Capability Index
- CCMP: Cyber Crisis Management Plan
- CII: Critical Information Infrastructure
- CMM: Cybersecurity Maturity Model
- CNAP: Calling Name Presentation
- CRA: Cyber Resilience Act
- DPDP: Digital Personal Data Protection
- EHR: Electronic Health Record
- GCC: Government Community Cloud
- GPAI: Global Partnership on Artificial Intelligence
- IaaS: Infrastructure as a Service
- MeitY: Ministry of Electronics and Information Technology
- MHA: Ministry of Home Affairs
- MSSP: Managed Security Service Provider
- NCSA: National Cyber Security Agency
- NCSC: National Cyber Security Centre
- NeGD: National e-Governance Division
- NSM: National Security Memorandum
- OECD: Organisation for Economic Cooperation and Development
- PCPD: Privacy Commissioner for Personal Data
- RAT: Remote Access Trojan
- RBI: Reserve Bank of India
- SaaS: Software as a Service
- SCAA: South China Athletic Association
- SEBI: Securities and Exchange Board of India
- SOC: Security Operations Centre
- SOHO: Small Office/Home Office
- SRMA: Sector Risk Management Authority

Sources

- **SEBI has Mandated SEBI-regulated Entities to Adopt the Cybersecurity and Cyber Resilience Framework**
  https://www.moneycontrol.com/
  https://www.sebi.gov.in/
- **Cyber Surakshit Bharat Initiative by MeiTy**
  https://www.meity.gov.in/
  https://opengovasia.com/
- **Global IndiaAI Summit 2024**
  https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2030838
- **Tackling Mobile Frauds in New Government's 100-day Plan**
  www.trai.gov.in/sites/default/files/Recommendation_23022024.pdf
  https://www.trai.gov.in/sites/default/files/PR_No.08of2024.pdf
  https://economictimes.indiatimes.com/
- **RBI's Supervisory Action Against Indian Bank**
  https://www.rbi.org.in/
- **NIST Released Product Development Cybersecurity Handbook**
  https://csrc.nist.gov/
  https://business.cch.com/
- **Open Source Foundations Unite on Common Standards for EU's Cyber Resilience Act**
  https://techcrunch.com/
- **CISA Launched High-Risk Communities Webpage**
  https://www.cisa.gov/
- **NCSC Released New Version of Cyber Assessment Framework**
  https://www.ncsc.gov.uk/
- **White House Released National Security Memorandum-22**
  https://www.whitehouse.gov/
  https://www.cisa.gov/
- **MITRE Systems Breached**
  https://www.securityweek.com/
- **SCAA Suffered Cyberattack**
  https://thecyberexpress.com/
  https://www.scaa.org.hk/
- **Metasploit Meterpreter Installed via Redis Server**
  https://asec.ahnlab.com/en/64034/
- **Venom RAT Targeted Multiple Sectors**
  https://socradar.io/
  https://www.acronis.com/
  https://thehackernews.com/
- **Cuttlefish Malware Infects Routers**
  https://www.bleepingcomputer.com/
- **Agenda Ransomware Propagates via Custom PowerShell Script**
  https://www.trendmicro.com/

- **MuddyWater Hackers Adopt New C2 Tool 'DarkBeatC2'**
  https://thehackernews.com/
- **ArcaneDoor - New Espionage-focused Campaign**
  https://blog.talosintelligence.com/
  https://www.darkreading.com/
- **Large-Scale StrelaStealer Campaign**
  https://unit42.paloaltonetworks.com/strelastealer-campaign/
- **Attack Surface Management vs. Vulnerability Management**
  https://thehackernews.com/
- **Managed Service Provider & Managed Security Service Provider**
  https://www.digitalocean.com/
  https://blog.ccasociety.com/
- **Critical Vulnerability in Palo Alto Networks**
  https://security.paloaltonetworks.com/CVE-2024-3400
- **Critical Vulnerability in xz Libraries**
  https://access.redhat.com/security/cve/CVE-2024-3094
  https://www.redhat.com/
- **Critical Vulnerability in CrushFTP**
  https://nvd.nist.gov/vuln/detail/CVE-2024-4040
  https://www.crushftp.com/index.html
- **New TunnelVision Attack Allows Hijacking of VPN Traffic**
  https://thehackernews.com/
- **CHAVELOAK: The Latest Banking Trojan Threat Targeting Brazil**
  https://www.fortinet.com/
- **Microsoft Alerts Users to "Dirty Stream" Attack**
  https://www.microsoft.com/
- **Android 'eXotic visit' Spyware**
  https://thehackernews.com/
- **The New Android Trojan SoumniBot Evade Detections**
  https://thehackernews.com/

National Critical Information Infrastructure Protection Centre

सत्यमेव जयते

NCIIPC

सम्पूर्ण सुरक्षा

A unit of NTRO

Feedback/Contribution

Suggestions, feedback and contributions are welcome at newsletter@nciipc.gov.in

Disclaimer

NCIIPC does not endorse any vendor, product or service. The content of the newsletter is for informational purpose only. Readers may validate the information on their own.