
# NCIIPC NEWSLETTER

# JANUARY 2025

National Critical Information Infrastructure Protection Centre

(A unit of National Technical Research Organisation)

National Critical Information Infrastructure Protection Centre
NCIIPC
सम्पूर्ण सुरक्षा
A unit of NTRO

# RELEASE OF NATIONAL CYBERSECURITY REFERENCE FRAMEWORK (NCRF)

The NCRF aims to provide essential guidelines for securing Critical Information Infrastructures


https://nciipc.gov.in/
@NCIIPC
NCIIPC India
NCIIPC India
helpdesk1@nciipc.gov.in
1800-11-4430

VOLUME 9 ISSUE 1


@NCIIPC

# NCIIPC Newsletter

January 2025


## Inside This Issue



## Message from the NCIIPC Desk

Dear Readers,

Best wishes from NCIIPC for year 2025. NCIIPC continues its effort to make our stakeholders more cyber security aware through our Newsletters in year 2025.

The National Cybersecurity Reference Framework (NCRF) was launched by Dy. NSA Sh. T V Ravichandran during Bharat NCX 2024. The NCRF aims to provide essential guidelines for securing critical information infrastructure. This will help establish robust cyber defences across various critical sectors.

NCIIPC was part of the 7th edition of the Smart India Hackathon (SIH) that was held concurrently at 51 nodal centres nationwide. The software edition ran nonstop for 36 hours and the hardware edition continued from 11 December 2024 to 15 December 2024, bringing together the brightest young minds to showcase innovative solutions. This initiative was spearheaded by the Ministry of Education's Innovation Cell.

In the last quarter, the Ministry of Electronics and Information Technology (MeitY) has called for project proposals in cybersecurity, focusing on innovation and the development of indigenous technologies that lead to productisation.

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.

# Policy & Strategy

**National Cybersecurity Reference Framework (NCRF)**

The National Security Council Secretariat (NSCS), through the Office of the National Cyber Security Coordinator (NCSC), and the National Critical Information Infrastructure Protection Centre (NCIIPC) have formulated the National Cybersecurity Reference Framework (NCRF). NCRF version has been prepared with inputs from stakeholders, including Critical Sector Ministries, Regulators, Critical Sector Entities and Cyber Security Experts from the academia as well as the industry from across the country. After studying and analysing various policies, guidelines, regulatory and industry best practices available worldwide, NCRF has come up with guidelines which is most relevant for the country and would be mandated or recommended to be adopted by different stakeholders, especially the Critical Sector Entities (CSEs), in our federated digital ecosystem. It gives cybersecurity practitioners a well-rounded perspective of the multi-dimensional aspects of cybersecurity and cyber resilience.

*After studying and analysing various policies, guidelines, regulatory and industry best practices available worldwide, NCRF has come up with guidelines which is most relevant for the country.*

**Bharat NCX 2024**

The Bharat National Cyber Exercise (NCX) 2024 has successfully concluded, setting a new benchmark for India's cybersecurity capabilities. With over 600 participants, including cybersecurity experts, policymakers, defence professionals, and academic leaders, the event fostered collaboration to enhance the nation's resilience against cyber threats. It provided a platform for strengthening India's cybersecurity frameworks. One of the key highlights of the event was the launch of the National Cybersecurity Reference Framework (NCRF). The NCRF aims to provide essential guidelines for securing critical infrastructure, ensuring organisations can improve their cyber defences across various sectors. Another significant development was the unveiling of the National Cyber Range 1.0 (NCR-1.0), developed by Rashtriya Raksha University (RRU). This indigenous platform has been designed to simulate cyberattacks, providing a secure environment for cybersecurity training and testing, thus enhancing India's self-reliance in this critical area. The Bharat CISOs Conclave and the Bharat Cybersecurity Startup Exhibition showcased cutting-edge innovations, marking India's growing influence in global cybersecurity. These efforts are pivotal to reinforcing the country's digital security infrastructure.


*Please refer page 22 & 23 for reference.*

# Trends

**Service Level Agreements in Cybersecurity**

*The goal of SLAs is to outline the specific services being provided, the expected level of performance, establish specific metrics to measure the performance of the service, and detail the consequences for failing to meet the agreed-upon standards/ expectations.*

Service Level Agreements (SLA) are formal agreements between a service provider and a client that define the expected level of service, including security measures and practices, that the provider will deliver. SLA agreements outline the specific obligations and responsibilities of both parties, such as uptime commitments, data protection measures, incident response times, and compliance with regulatory standards. The goal of SLAs is to outline the specific services being provided, the expected level of performance, establish specific metrics to measure the performance of the service, and detail the consequences for failing to meet the agreed-upon standards/expectations. Security and compliance are key components of an SLA. Integrating cybersecurity into SLAs ensures that both service provider and client understand and agree upon the security measures necessary to protect sensitive information such as data protection, incident response, access controls, regular security assessment, and compliance with regulatory requirements. The purpose of the SLA process is to set clear expectations and standards for the security of systems and data managed by the service provider. This includes outlining specific security protocols and practices, defining acceptable risk levels, and specifying procedures for incident detection and response. By establishing these parameters, SLAs provides a basis for accountability and transparency in the provider-client relationship, helping to build trust and facilitate a more secure and reliable service experience.

**Benefits of AI in Cybersecurity**

*Some AI-powered tools can process security alerts and offer users step-by-step remediation instructions based on input from the user, resulting in more effective and tailored remediation recommendations.*

Cybersecurity presents unique challenges, including a constantly evolving threat landscape, and vast attack surface. Since AI can analyse massive volumes of data, identify patterns that humans might miss, and adapt and improve its capabilities over time, it has significant benefits when applied to cybersecurity. Threat detection is one of the most common applications of AI in cybersecurity. Another top application of AI in cybersecurity is threat management. AI is also used effectively to automate certain actions to speed up incident response times.

Latest developments in cybersecurity using AI:

AI-powered remediation: More advanced applications of AI can help security teams to remediate threats faster and easier. Some AI-powered tools can process security alerts and offer users step-by-step remediation instructions based on input from the user, resulting in more effective and tailored remediation recommendations.

*Please refer page 22 & 23 for reference.*

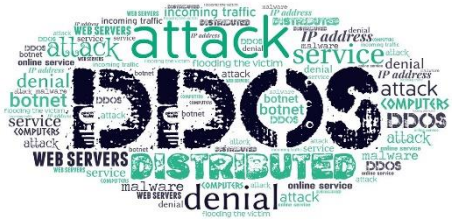
Enhanced threat intelligence using generative AI: Generative AI is increasingly being deployed in cybersecurity solutions to transform how analysts work. Rather than relying on complex query languages, operations, and reverse engineering to analyse vast amounts of data to understand threats, analysts can rely on generative AI algorithms that automatically scan code and network traffic for threats and provide rich insights.

**GitHub, Telegram Bots, and ASCII QR Codes Abused in Phishing Attacks**

A new wave of phishing attacks is leveraging GitHub repositories, Telegram bots, and ASCII QR codes. Malicious scripts are hosted on GitHub, while Telegram bots facilitate communication and data theft. QR codes in phishing messages redirect users to fraudulent websites. This approach helps attackers evade detection, boosting their ability to steal sensitive data like credentials. The campaign uses trusted platforms to conduct cyber attacks, making it difficult for security measures to block. Victims are increasingly targeted through unconventional, yet effective, phishing methods. The rise of these tactics highlights the increasing sophistication of cyber attacks.


**Cybersecurity firm Defends Against Record-Breaking 3.8 Tbps DDoS Attack Targeting Critical Sectors**

The recent surge in Distributed Denial-of-Service (DDoS) attacks, highlights the growing threat of large-scale cyberattacks on organisations across various sectors, including financial services, and telecommunications. One cybersecurity firm reported that it successfully mitigated a record-breaking DDoS attack, which peaked at 3.8 terabits per second (Tbps) and lasted for 65 seconds. These attacks are often based on the User Datagram Protocol (UDP), which is a connectionless protocol easily exploited for amplification attacks. UDP's lack of connection management allows attackers to generate high packet rates, overwhelming target networks by consuming bandwidth and CPU resources, which can prevent legitimate users from accessing services. In this particular case, the DDoS attack was powered by a large botnet of ASUS home routers, which were infected using a vulnerability (CVE-2024-3080) with a critical CVSS score of 9.8.




*UDP's lack of connection management allows attackers to generate high packet rates, overwhelming target networks by consuming bandwidth and CPU resources, which can prevent legitimate users from accessing services.*

The use of DNS-over-HTTPS (DoH) for Command and Control (C2) communications adds a layer of complexity to DDoS mitigation, as DoH traffic is encrypted and can blend in with legitimate web traffic, making it harder for defenders to differentiate between malicious and normal communications. This evolving tactic highlights the need for enhanced monitoring and filtering solutions to inspect encrypted DNS traffic for malicious patterns.

*Please refer page 22 & 23 for reference.*

Furthermore, a significant concern arises from the recently discovered CUPS vulnerability (CVE-2024-47176) in Linux-based systems. This flaw allows attackers to exploit CUPS (Common UNIX Printing System) services to achieve a 600x amplification in just a few seconds, making it a potent vector for DDoS attacks. With 7,171 exposed hosts vulnerable to this issue, many organisations unknowingly contribute to the DDoS ecosystem, amplifying the scale of these attacks. As a result, organisations are advised to remove or disable CUPS services if printing functionality is not essential.

*To defend against such high-volume DDoS attacks, organisations must adopt effective mitigation strategies, such as packet inspection and filtering, to discard malicious traffic while preserving enough CPU capacity for legitimate requests.*

To defend against such high-volume DDoS attacks, organisations must adopt effective mitigation strategies, such as packet inspection and filtering, to discard malicious traffic while preserving enough CPU capacity for legitimate requests. Given the use of DoH for C2, it's also crucial to implement DNS filtering solutions capable of detecting and blocking malicious DNS queries. Organisations must remain vigilant about emerging vulnerabilities, implement proactive patch management, and regularly review the necessity of services like CUPS to minimise their exposure to these growing DDoS threats.

## Malware Bytes

**Researchers Discover first UEFI Bootkit Malware for Linux**

*Though not yet deployed in real-world attacks, the emergence of Bootkitty highlights the growing sophistication of threats targeting Linux, a platform often seen as more secure or less vulnerable.*

A new UEFI bootkit, named Bootkitty, has been discovered as the first specifically targeting Linux systems, signaling a shift in bootkit threats that have historically focused on Windows. While Bootkitty is currently a proof-of-concept, it demonstrates the potential for advanced malware to exploit vulnerabilities in Linux systems, particularly on certain Ubuntu versions and configurations. Unlike typical malware, bootkits operate at the firmware level, providing stealthy, hard-to-remove access to compromised systems, making them a significant security threat. Though not yet deployed in real-world attacks, the emergence of Bootkitty highlights the growing sophistication of threats targeting Linux. This discovery suggests that attackers could increasingly focus on Linux environments, which are widely used in critical infrastructure, servers, and secure applications. The ability to compromise the boot process allows for persistent access and evasion of detection, posing significant risks to sensitive systems.

**Linux Variant of FASTCash Malware Targeted Payment Switches in ATM**

It has been observed in USA that threat actors are using a Linux variant of a well-known malware family called FASTCash in a financially-motivated campaign. The FASTCash malware is

*Please refer page 22 & 23 for reference.

specifically designed to target payment switches within compromised networks that process card transactions. The malware facilitates the unauthorised withdrawal of cash from ATMs by exploiting vulnerabilities in the systems handling these transactions.

*The malware facilitates the unauthorised withdrawal of cash from ATMs by exploiting vulnerabilities in the systems handling these transactions.*

Key points about the FASTCash Linux variant:

Targeting Payment Switches: The malware is deployed on payment switch systems that manage the communication between ATMs, banking networks, and other financial institutions. These switches are integral to the card transaction process.

ATM Cash Withdrawals: Once the malware is installed, it allows the attackers to bypass security protocols, enabling them to make unauthorised withdrawals from ATMs, potentially draining funds from targeted bank accounts.

Financial Motivation: The campaign appears to be part of a financially-driven effort, likely aimed at stealing large sums of money, which is consistent with previous attacks attributed to this threat actor.

**Salt Typhoon Hackers Backdoor Telcos with GhostSpider Malware**

The'Salt Typhoon' threat actor was observed using a new "GhostSpider" backdoor in attacks targeting telecommunication service providers. GhostSpider backdoor is designed for long-term espionage operations requiring high levels of stealth, achieved through encryption and residing solely in memory. The backdoor is loaded on the target system using DLL hijacking and registered as a service via the legitimate 'regsvr32.exe' tool, while a secondary module loads encrypted payloads directly in memory. GhostSpider executes commands received from the command and control (C2) server, concealed within HTTP headers or cookies to blend with legitimate traffic.

*GhostSpider backdoor is designed for long-term espionage operations requiring high levels of stealth, achieved through encryption and residing solely in memory.*

**Fake AI Video Generators Infect OS with Infostealers**

Fake AI image and video generators are being used to distribute Lumma Stealer and AMOS malware, targeting Windows and macOS systems, respectively. These information-stealing malware variants are designed to steal sensitive data, including cryptocurrency wallets, credentials, passwords, credit card information, cookies, and browsing history from popular browsers like Google Chrome, Microsoft Edge and Mozilla Firefox. Once installed, the malware collects the data and compiles it into an archive, which is then sent back to the attacker. The stolen information can be used for identity theft, financial fraud, phishing attacks or sold on cyber crime marketplaces. The

*The malware is primarily spreads through fake AI tools, targeting users seeking content creation software. This highlights the growing threat of socially engineered attacks exploiting popular interests to distribute malware.*

*Please refer page 22 & 23 for reference.*

malware primarily spreads through fake AI tools, targeting users seeking content creation software. This highlights the growing threat of socially engineered attacks exploiting popular interests to distribute malware. To protect against such threats, users should avoid downloading software from untrusted sources, keep security software updated, and use strong passwords along with two-factor authentication where possible.

**Malware Campaign Delivered DarkVision RAT**

*Key capabilities of DarkVision RAT include Keylogging, Remote Access, Password Theft, Audio Recording and Screen Capturing.*

The recent disclosure of a new malware campaign highlights the use of PureCrypter, a malware loader, to deliver a Remote Access Trojan (RAT) called DarkVision RAT. The DarkVision RAT utilises a custom network protocol for communication with its Command and Control (C2) server via sockets. This design is intended to enhance the malware's stealth and resilience against detection. Key capabilities of DarkVision RAT include Keylogging, Remote Access, Password Theft, Audio Recording and Screen Capturing. These features make DarkVision RAT a versatile and dangerous tool for cyber criminals, enabling them to maintain control over infected systems, exfiltrate data, and escalate their malicious activities. The use of PureCrypter to load this RAT suggests a sophisticated malware campaign designed to evade traditional security measures, particularly by obfuscating the malicious payload and complicating detection efforts.

**Gorilla Botnet for DDoS Attacks**

*The botnet primarily conducts DDoS attacks, targeting sectors like government websites, banks, and telecom.*

Cybersecurity researchers have reported botnet malware family named Gorilla (also known as GorillaBot). This botnet appears to be inspired by the Mirai botnet, which gained notoriety for using Internet of Things (IoT) devices to launch large-scale Distributed Denial of Service (DDoS) attacks. The botnet primarily conducts DDoS attacks, targeting sectors like government websites, banks, and telecom. GorillaBot likely exploits IoT devices with weak or default credentials, similar to Mirai. Its attacks employ various methods such as SYN floods, UDP floods, and HTTP floods, causing significant disruption. The botnet operates through a Command & Control (C&C) infrastructure, remotely directing infected devices. With its high attack density and widespread impact, GorillaBot poses a severe risk to both service availability and critical sectors. Mitigating its effects requires robust DDoS defences and securing IoT devices to prevent exploitation.

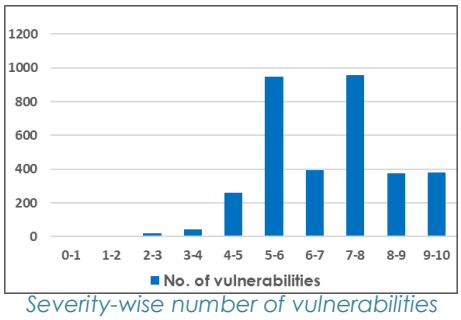
*Please refer page 22 & 23 for reference.*

# Vulnerability Watch

### Quarterly Vulnerability Analysis Report

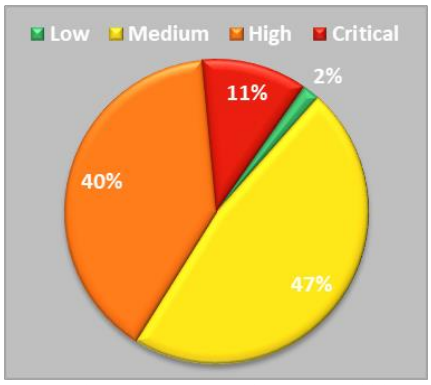
*Alert & Advisory Group, NCIIPC*

The cyber security trends have suggested surge in critical vulnerabilities & exploits in the quarter impacting widely used software and cloud services. During the last quarter of 2024, a total of 3372 vulnerabilities have been observed. More than 50 percent of total vulnerabilities reported were of Critical & high severity. Linux, Apple, Microsoft, Adobe and Google were the top five vendors having 36% of total reported vulnerabilities. The CVEs have various impact for organisations in critical sectors and require vigilance by relevant SOC/IT teams for patch management & cybersecurity measures.



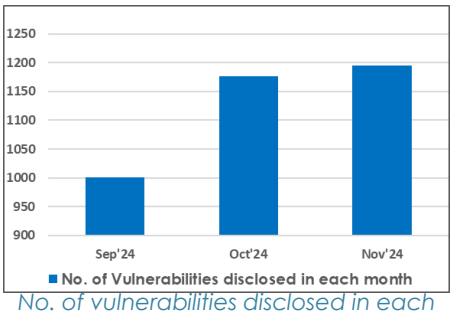

*Severity-wise number of vulnerabilities*

| Severity | CVSS v3 Score | Number of Vulnerabilities | | | Total Vulnerabilities | Severity Total |
|---|---|---|---|---|---|---|
| | | Sep'24 | Oct'24 | Nov'24 | | |
| Critical | 10-9 | 118 | 128 | 133 | 379 | 379 |
| High | 9-8 | 83 | 142 | 151 | 376 | 1334 |
| | 8-7 | 285 | 272 | 401 | 958 | |
| Medium | 7-6 | 134 | 149 | 109 | 392 | 1596 |
| | 6-5 | 277 | 378 | 291 | 946 | |
| | 5-4 | 85 | 83 | 90 | 258 | |
| Low | 4-3 | 12 | 14 | 18 | 44 | 63 |
| | 3-2 | 7 | 10 | 2 | 19 | |
| | 2-1 | 0 | 0 | 0 | 0 | |
| | 1-0 | 0 | 0 | 0 | 0 | |
| Total | | 1001 | 1176 | 1195 | | 3372 |

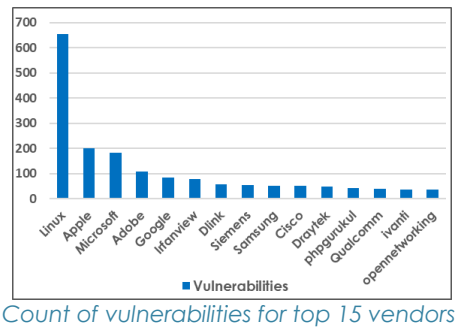



*Severity-wise share of vulnerabilities*

| S. No. | Vendor | No. of Vulnerabilities | | | Total |
|---|---|---|---|---|---|
| | | Sep'24 | Oct'24 | Nov'24 | |
| 1. | Linux | 124 | 327 | 202 | 653 |
| 2. | Apple | 96 | 70 | 33 | 199 |
| 3. | Microsoft | 53 | 25 | 104 | 182 |
| 4. | Adobe | 23 | 33 | 52 | 108 |
| 5. | Google | 23 | 29 | 32 | 84 |
| 6. | Irfanview | 0 | 0 | 77 | 77 |
| 7. | Dlink | 13 | 26 | 18 | 57 |
| 8. | Siemens | 3 | 22 | 29 | 54 |
| 9. | Samsung | 32 | 0 | 18 | 50 |
| 10. | Cisco | 2 | 48 | 0 | 50 |
| 11. | Draytek | 38 | 4 | 5 | 47 |
| 12. | phpgurukul | 11 | 18 | 13 | 42 |
| 13. | Qualcomm | 13 | 1 | 24 | 38 |
| 14. | Ivanti | 17 | 2 | 18 | 37 |
| 15. | opennetworking | 37 | 0 | 0 | 37 |




*No. of vulnerabilities disclosed in each month*




*Count of vulnerabilities for top 15 vendors*

*Please refer page 22 & 23 for reference.*

*Though not yet deployed in real-world attacks, the emergence of Bootkitty highlights the growing sophistication of threats targeting Linux, a platform often seen as more secure or less vulnerable. CVE IDs areCVE-2024-0012 & CVE-2024-9474*

**Palo Alto Networks Devices Hacked**

A major cyberattack has affected around 2,000 Palo Alto Networks devices, exploiting two critical vulnerabilities: CVE-2024-0012 (authentication bypass, CVE score 6.9) and CVE-2024-9474 (privilege escalation, CVSS score 9.3). These flaws allow attackers to modify device configurations and execute arbitrary code, enabling command execution and malware deployment, such as PHP web shells. A large number of firewalls (13,324) have publicly exposed management interfaces, although not all of them are vulnerable. The exploitation of these vulnerabilities has intensified, particularly after a proof-of-concept exploit combining both flaws was publicly released. Palo Alto Networks has advised its customers to secure their firewalls' management interfaces by restricting access to the internal network.

*The flaw was identified using AI-generated fuzz targets which enhance fuzzing coverage across 272 C/C++ projects. This AI-assisted method helped find vulnerabilities that traditional fuzzing might have missed, including one present in the OpenSSL codebase for nearly 20 years. CVE ID is CVE-2024-9143*

**Google's AI-Powered Tool Discovered Vulnerabilities in OpenSSL**

Google's AI-powered fuzzing tool, OSS-Fuzz, has discovered 26 vulnerabilities in open-source projects, including a medium-severity flaw in OpenSSL (CVE-2024-9143). This memory write bug could lead to application crashes or remote code execution but has been patched in multiple OpenSSL versions. The flaw was identified using AI-generated fuzz targets which enhance fuzzing coverage across 272 C/C++ projects. This AI-assisted method helped find vulnerabilities that traditional fuzzing might have missed, including one present in the OpenSSL codebase for nearly 20 years. In addition to fuzzing, Google is moving its codebases to memory-safe languages like Rust and improving C++ projects such as Chrome. The company has implemented safer coding techniques like Safe Buffers and a hardened version of libc++, which adds bounds checking to prevent spatial memory safety bugs with minimal performance impact. These initiatives aim to improve software security and reliability, ensuring that vulnerabilities are detected and mitigated more effectively while maintaining performance and functionality.

*The RCE vulnerability arises due to improper authorisation and insufficient information, allowing attackers to exploit it remotely and execute arbitrary code on the affected systems. CVE ID is CVE-2024-43602*

**Critical Vulnerability in Microsoft Azure CycleCloud**

A critical Remote Code Execution (RCE) vulnerability, having CVE ID CVE-2024-43602 and CVSS score of 9.9, has been discovered in Microsoft Azure CycleCloud. This flaw affects Azure CycleCloud versions 8.0.0 to 8.6.5. The RCE vulnerability arises due to improper authorisation and insufficient information, allowing attackers to exploit it remotely and execute arbitrary code on the affected systems. The vulnerability poses significant security risks to users of these versions of Azure CycleCloud. However, Microsoft has already issued a patch to resolve the issue, ensuring that systems are protected from this vulnerability. The vendor has also provided guidance on how to remediate the flaw and prevent further

*Please refer page 22 & 23 for reference.*

exploitation. Users are encouraged to apply the patch as soon as possible to safeguard their systems.

**Critical Vulnerabilities in Siemens Products**

A critical Path Traversal vulnerability has been identified in Siemens SINEC INS. The flaw occurred because the application failed to properly sanitise user-provided paths during SFTP-based file uploads and downloads. This allows authenticated remote attackers to manipulate arbitrary files on the system, potentially leading to arbitrary code execution on the device. The Path Traversal vulnerability has CVE ID CVE-2024-46888 with CVSS score of 9.4. It affects all versions of SINEC INS before V1.0 SP2 Update 3. If exploited, attackers could execute arbitrary code and compromise the device. Siemens has issued a patch to address the vulnerability, and affected users are strongly advised to update to the latest version to mitigate the risk.

*The Path Traversal vulnerability has CVE ID CVE-2024-46888. It affects all versions of SINEC INS before V1.0 SP2 Update 3.*

Also another critical Argument Injection vulnerability has also been discovered in Siemens SINEC Security Monitor. This flaw occurs due to improper validation of user input in the ssmctl-client command. This allows an authenticated attacker with low privileges to execute arbitrary code with root privileges on the underlying operating system. The vulnerability has been assigned a CVSS score of 9.4 having CVE ID CVE-2024-47553. Siemens has released a patch to address this issue.

*The Path Traversal vulnerability has CVE ID CVE-2024-46888 with CVSS score of 9.4.*

**Critical Vulnerability in WordPress AR**

A critical Arbitrary File Upload vulnerability has been discovered in the AR for WordPress plugin, allowing unrestricted file uploads of dangerous types. This flaw enables attackers to upload malicious files, such as web shells, to the web server, potentially gaining full control of the system. The vulnerability has been assigned a CVE ID CVE-2024-50496 having CVSS score of 10.0. The flaw affects versions of the AR for WordPress plugin up to version 6.2. If exploited, attackers can upload malicious files, such as web shells, which could lead to the compromise of the affected server. This puts websites at significant risk of unauthorised access and control by attackers. To mitigate this issue, users are strongly advised to update their AR for WordPress plugin to the latest version, which addresses the vulnerability. Ensuring that all systems are up-to-date is critical to protecting against potential attacks exploiting this flaw.

*To mitigate this issue, users are strongly advised to update their AR for WordPress plugin to the latest version, which addresses the vulnerability. CVE ID is CVE-2024-50496*

**Critical Vulnerability in Cisco**

A critical Command Injection vulnerability has been discovered in Cisco Secure Firewall Management Center (FMC) Software. This flaw allows an authenticated remote attacker to execute

*Please refer page 22 & 23 for reference.*

arbitrary commands with root privileges on the underlying operating system. This occurs due to insufficient input validation of certain HTTP requests. To exploit the vulnerability, an attacker must first authenticate to the web-based management interface and send a crafted HTTP request. If successfully exploited, this vulnerability could grant the attacker root access on both the FMC and managed Cisco Firepower Threat Defense (FTD) devices. The CVE ID is CVE-2024-20424 and CVSS score for this vulnerability is 9.9. This flaw presents a serious security risk, as it could allow attackers to execute commands with elevated privileges, potentially compromising the integrity of the entire system. Cisco has advised users to apply necessary patches to mitigate the risk.

*This flaw allows an authenticated remote attacker to execute arbitrary commands with root privileges on the underlying operating system. CVE ID is CVE-2024-20424*

**Critical Vulnerability in Camaleon CMS**

A critical arbitrary file write vulnerability has been identified in Camaleon CMS, a Ruby on Rails-based content management system. The flaw, located in the MediaController's file upload method, allows authenticated users to write arbitrary files to any location on the server. If a malicious user uploads a Ruby file to the config/initializers/ directory, it could lead to remote code execution. The vulnerability has been assigned CVE ID CVE-2024-46986 and CVSS score of 9.9. Users are advised to upgrade to version 2.8.2, where the issue has been fixed.

*The flaw, located in the MediaController's file upload method, allows authenticated users to write arbitrary files to any location on the server. CVE ID is CVE-2024-46986*

**Critical Vulnerability in macOS**

A critical vulnerability was found in macOS versions prior to 15, which allowed an app to potentially escape its sandbox due to inadequate validation of file attributes. This flaw was assigned CVE ID CVE-2024-44148 and CVSS score of 10.0. The issue could have enabled unauthorised access to the system, posing a significant security risk. The vulnerability has been addressed in macOS Sequoia 15, where improvements were made to the validation of file attributes, preventing potential sandbox escape.

**Critical Vulnerability in FreeBSD**

A critical vulnerability has been discovered in FreeBSD (a free and open-source Unix-like operating system), which allows a malicious actor to exploit concurrent removals of anonymous shared memory mappings, leading to premature object free. This issue occurs when the UMTX_SHM_DESTROY sub-request is used in parallel, potentially resulting in a kernel panic, Use-After-Free attacks, or enabling an attacker to execute code or escape a Capsicum sandbox. The vulnerability has CVE ID CVE-2024-43102 and CVSS score of 10.0. If successfully exploited, this flaw can allow attackers to compromise system stability, escalate privileges, or bypass security protections. Users are advised to upgrade to patched versions to mitigate the risk.

*If successfully exploited, this flaw can allow attackers to compromise system stability, escalate privileges, or bypass security protections. CVE ID is CVE-2024-43102*

*Please refer page 22 & 23 for reference.*

# News Snippets - National

**First Cyber Policy Dialogue Between India and Singapore**

The First Cyber Policy Dialogue between India and Singapore took place on 17th October 2024 in Singapore, co-chaired by Sh. Amit A. Shukla, Joint Secretary of Cyber Diplomacy from India's Ministry of External Affairs, and Sh. David Koh, Chief Executive of Singapore's Cyber Security Agency. The dialogue aimed to strengthen bilateral cooperation in cybersecurity by discussing key topics such as the global cyber threat landscape, national cyber strategies, and evolving cyber governance under the United Nations. Both nations shared insights on cyber threat assessments and explored ways to collaborate on cyber threat alerts, responses, and protecting Critical Information Infrastructure. They also discussed the exchange of best practices and knowledge, focusing on building joint capacity and organising training activities to enhance cyber defense capabilities. This dialogue marks a significant step in fostering deeper cybersecurity collaboration between India and Singapore, with both countries committed to addressing emerging cyber risks and building resilient digital infrastructures. The discussions lay the foundation for continued partnership in tackling cybersecurity challenges on a global scale.

*The dialogue aimed to strengthen bilateral cooperation in cybersecurity by discussing key topics such as the global cyber threat landscape, national cyber strategies, and evolving cyber governance under the United Nations.*

**MeitY Call for Project Proposals in Cyber Security**

The Ministry of Electronics and Information Technology (MeitY) has called for project proposals in cybersecurity, focusing on innovation and the development of indigenous technologies that lead to productisation. The initiative aims to strengthen India's cybersecurity capabilities by encouraging the creation of homegrown solutions to address the growing cyber threat landscape. Proposals were invited in specific thrust areas outlined by MeitY, with an emphasis on practical, scalable technologies that can enhance the nation's cybersecurity infrastructure. The goal is to foster research and development that not only boosts national security but also contributes to India's technological self-reliance. This call for proposals is part of India's broader strategy to build a secure and resilient digital ecosystem, encouraging the development of indigenous products to safeguard critical digital assets. MeitY is looking for projects that offer actionable, deployable solutions, with a focus on both innovation and real-world applicability. The initiative aligns with the government's vision to strengthen digital infrastructure and position India as a leader in cybersecurity innovation.

*The initiative aims to strengthen India's cybersecurity capabilities by encouraging the creation of homegrown solutions to address the growing cyber threat landscape.*

*Please refer page 22 & 23 for reference.*

# News Snippets - International

**Australia to Mandate Reporting of Ransomware Payments**

Australia has taken a significant step in the fight against cybercrime with the introduction of a new law that requires businesses to report any payments made in response to ransomware attacks. The Cyber Security Bill 2024, introduced to the Australian Federal Parliament, aims to combat the growing threat of ransomware and increase transparency around extortion payments. The bill mandates that businesses with an annual turnover above AU$3 million must report any ransomware payments to the Department of Home Affairs. This move comes after several high-profile cyberattacks, including breaches involving Optus, Medibank and MediSecure. These incidents have highlighted the urgent need for stronger cybersecurity measures in the country. Under the proposed law, businesses are required to report ransomware payments within 73 hours, or face fines of up to AU$18,000. The government hopes this will help provide greater insight into the financial impact of ransomware attacks, with Cybersecurity Minister Tony Burke noting that Australian businesses paid an average of AU$9.27 million in ransom in 2023. In addition to the reporting requirement, the bill includes new security standards for smart devices, stronger cooperation between government and industry, and the creation of a Cyber Incident Review Board to investigate significant cyber events. This legislation marks a pivotal moment in Australia's approach to cybersecurity and aims to better protect businesses and individuals from the escalating threat of ransomware.

*Under the proposed law, businesses are required to report ransomware payments within 73 hours, or face fines of up to AU$18,000.*

**Google Cloud to Require Multi-Factor Authentication by 2025**

Google has announced that by the end of 2025, Multi-Factor Authentication (MFA) will be mandatory for all users of Google Cloud services. This new policy is part of an effort to strengthen security for Google Cloud accounts, including those of admins and users with access to cloud resources. It will not affect personal Google accounts. The MFA rollout will occur in three stages. Beginning this month, users who haven't enabled MFA will receive reminders to do so, as approximately 30% of Google Cloud users are still without this added security feature. In early 2025, all users who only rely on passwords to sign in will be prompted to set up MFA for platforms like the Google Cloud Console and Firebase Console. By the end of 2025, MFA will be a requirement for all users, including those accessing through federated identity providers.

*This new policy is part of an effort to strengthen security for Google Cloud accounts, including those of admins and users with access to cloud resources.*

**Free ISP Data Breach Exposed Personal Information**

French telecommunications provider 'Free' has confirmed a significant data breach that exposed the personal information of 19

*Please refer page 22 & 23 for reference.

million customers. The cyberattack involved unauthorised access to Free's internal management tool. The hacker, known as "drussellx," reportedly stole two databases containing sensitive data, including information on more than 5 million international bank accounts, and attempted to sell it on a Dark Web cybercrime forum. While Free assured customers that no passwords, bank card details, emails, SMS or voicemails were compromised, the breach still raises concerns about the security of personal data. Free serves over 22 million mobile and fixed-line subscribers and has stated that its services were not impacted by the attack. The company has already filed a criminal complaint and reported the incident to France's National Commission for Information Technology and Civil Liberties (CNIL) and the National Agency for the Security of Information Systems (ANSSI).

*The cyberattack involved unauthorised access to Free's internal management tool.*

**PSAUX Ransomware Targets Over 22,000 CyberPanel Servers**

A widespread ransomware attack has impacted over 22,000 servers running CyberPanel, a popular web hosting management platform. The attack, attributed to the PSAUX ransomware group, exploits a critical security flaw in CyberPanel versions 2.3.6 and potentially 2.3.7, which allows attackers to remotely execute commands without authentication. This vulnerability stems from issues in authentication processes, improper sanitisation of user inputs, and flaws in the security filters, leaving servers exposed to exploitation. The PSAUX ransomware encrypts files on affected servers, appending a ".psaux" extension to encrypted files and placing ransom notes in multiple locations. At the time of the attack, over 152,000 domains and databases were under threat, as CyberPanel is often used to manage large-scale server environments. In response to the attack, CyberPanel's developers quickly released an emergency patch (version 2.3.8), which addresses the security vulnerabilities. Users are urged to upgrade their systems immediately to the latest version to mitigate further risk. A decryption tool has been made available for those impacted, though caution is advised when using it to avoid data corruption. To secure their servers, all CyberPanel users should upgrade to the latest version and follow the provided security guidance.

*The PSAUX ransomware encrypts files on affected servers, appending a ".psaux" extension to encrypted files and placing ransom notes in multiple locations.*

**Mobile and IoT Cyber Threats on the Rise**

Zscaler's newest ThreatLabz report reveals a worrying increase in mobile and IoT cyber threats, signaling growing challenges for businesses. From June 2023 to May 2024, mobile spyware attacks skyrocketed by 111% and banking malware rose by 29%. Many of these attacks are able to bypass multi-factor authentication (MFA), highlighting significant security gaps. IoT attacks also grew

*Please refer page 22 & 23 for reference.*

*Many of these attacks are able to bypass multi-factor authentication (MFA), highlighting significant security gaps.*

by 45%, with the manufacturing sector seeing the highest number of incidents. The report highlights another pressing issue: vulnerabilities in Operational Technology (OT) systems. Many of these systems still rely on outdated software, making them prime targets for cybercriminals. As OT systems become more interconnected with enterprise networks, the risk of breach escalates. To counter these threats, Zscaler recommends adopting a Zero Trust security approach. This strategy ensures secure, granular access to critical devices and systems, limiting the potential damage from any single breach. With cyber threats evolving rapidly, it's crucial for businesses to stay ahead by strengthening their security frameworks.

## Mobile Security

**TrickMo Banking Trojan Evolves: Steals Android PINs and Unlock Patterns**

*TrickMo can remotely control infected devices, steal SMS-based one-time passwords (OTPs), and use overlay screens to capture credentials by exploiting Android's accessibility services.*

Cybersecurity experts have issued a fresh warning about the TrickMo banking trojan, a malware strain infamous for targeting Android devices. TrickMo has evolved its tactics, now enabling attackers to capture sensitive data like Android PINs and unlock patterns. This development marks a significant escalation in its capabilities, posing a heightened threat to mobile banking users worldwide. TrickMo can remotely control infected devices, steal SMS-based one-time passwords, and use overlay screens to capture credentials by exploiting Android's accessibility services. Some of the new variants of the malware are designed to capture the device's unlock pattern or PIN by showing the victim a fake User Interface (UI) that closely resembles the actual unlock screen. This UI is an HTML page hosted on an external website and displayed in full-screen mode, creating the illusion of a genuine unlock screen. Another key feature of TrickMo is its wide-reaching targeting, collecting data from a diverse range of applications, including those related to banking, enterprise, job recruitment, e-commerce, trading, social media, streaming, entertainment, VPNs, government, education, telecom, and healthcare.

**Google Stopped Sideloading of Unsafe Android Apps**

Google has introduced a new security initiative in India that automatically blocks the sideloading of potentially harmful Android apps. This feature, designed to offer improved fraud protection, aims to safeguard users attempting to install malicious apps from non-Google Play Store sources, including web browsers, messaging apps, and file managers. Launched in Singapore earlier this year, the program has already prevented almost 900,000 risky installations in the country, according to Google. Eugene

*Please refer page 22 & 23 for reference.*

Liderman, Google's director of mobile security strategy, explained that this enhanced protection automatically detects and blocks apps that misuse sensitive permissions commonly exploited in financial fraud. The system operates by analysing the permissions specified by a third-party app in real time, looking for those commonly exploited by harmful apps to access SMS messages, notifications, and use accessibility services for overlays or other malicious activities. If any of these permissions are listed in the app's manifest ("AndroidManifest.xml") file, Google Play Protect will step in and automatically prevent the app from being installed on the user's Android device.

**SpyLoan: A Global Cyber Threat Fueled by Social Engineering**

SpyLoan apps are deceptive financial tools posing as quick loan providers with low interest rates and minimal requirements. They lure users through aggressive marketing, featuring countdowns and time-sensitive offers to create a false sense of urgency. However, their true motive lies in collecting vast amounts of personal data. Once installed, these apps demand intrusive permissions, accessing personal information, contacts, and sensitive device data. This information is then exploited to harass users into paying predatory interest rates. Victims are often subjected to relentless threats and privacy violations, creating a cycle of debt and emotional distress. Rather than offering genuine financial assistance, SpyLoan apps are designed to manipulate and extort users. They represent a growing global threat, exploiting the vulnerabilities of those in urgent need of financial aid. To protect yourself, research financial apps thoroughly, restrict app permissions to only necessary data, and report suspicious applications to authorities. Awareness and caution are the first steps in safeguarding against such schemes.

*Once installed, these apps demand intrusive permissions, accessing personal information, contacts, and sensitive device data.*

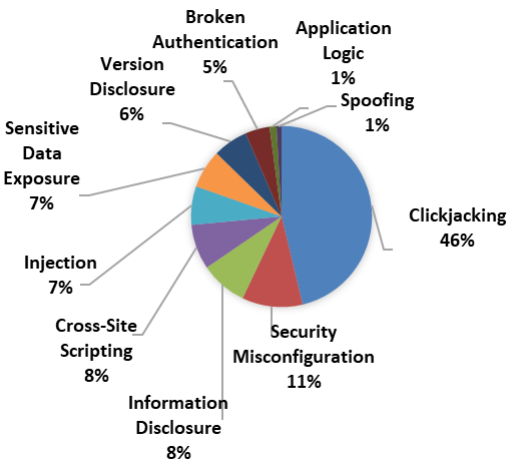
## NCIIPC Initiatives

**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 1837 vulnerabilities reported during the last quarter of 2024. The top 10 vulnerabilities are:

- Clickjacking
- Security Misconfiguration
- Information Disclosure
- Cross-Site Scripting

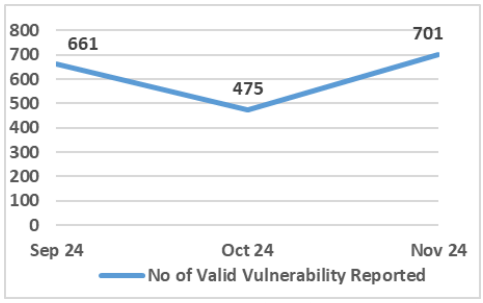
*Please refer page 22 & 23 for reference.*




- Injection
- Sensitive Data Exposure
- Version Disclosure
- Broken Authentication
- Application Logic
- Spoofing

Around 487 security researchers participated in RVDP programme during the last quarter of 2024. NCIIPC acknowledges following top 15 researchers for their contributions (names are in alphabetical order):

- Aaditya Wadodkar
- Aditya
- Anand Kumar Choubey
- Arit Dutta
- Dinesh N
- Hrishivaran S
- Karthik
- Keerthana.K
- Kiran Nandkumar Jagtap
- Lohit Koushik
- Manjot Singh
- No Name
- No Name
- Prasad R Sonar
- Vignesh Kj




*Last three months' timeline chart for vulnerabilities reported*

**NCIIPC at National Workshop on eOffice and eOffice Analytics Dashboard**

*Sh. Navin Kumar Singh, DG NCIIPC at DARPG Cyber Security workshop*

The Department of Administrative Reforms and Public Grievances (DARPG) organised a workshop on eOffice and eOffice Analytics Dashboard on 29th October, 2024 at CSOI Vinay Marg, New Delhi. Around 170 officials from 84 Ministries/Departments of the Central Government attended the workshop. Sh. Navin Kumar Singh, DG, NCIIPC, was one of the keynote speakers at the workshop. He advocated cyber vigilance and resilience by using simple measures that can have incremental changes in securing the e-office cyber space. He also emphasised on the importance of cyber hygiene culture.

*Please refer page 22 & 23 for reference.*

**NCIIPC at C0c0n 2024**


The C0c0n 2024 conference was held at Gandhinagar from 13th to 16th November 2024. Sh. Navin Kumar Singh Director General, NCIIPC and Sh. Len Noe, Transhuman, Cyborg Hacker & Technical Evangelist, CyberArk Software were the keynote speakers. NCIIPC was also part of the panel in "Transitioning from CTF to Real-World VAPT" at C0c0n 2024 conference.

**NCIIPC at ICCC2024**

The International Conference on Cyberlaw, Cybercrime & Cyber Security 2024 (ICCC2024) was organised by Cyberlaws.Net and Pavan Duggal Associates, Advocates, Supreme Court of India. The International Conference was attended by various international delegates and speakers. The ICCC2024 conference was held 13th to 15th November 2024. Sh. Tanay Bhattacharya, DDG NCIIPC, was one of the speakers in the conference. He addressed the challenges and opportunities in the ever-evolving landscape of cyber law, cybercrime, and cybersecurity.

*Please refer page 22 & 23 for reference.*


**JANUARY 2025**

| S | M | T | W | T | F | S |
|---|---|---|---|---|---|---|
| | | | 1 | 2 | 3 | 4 |
| 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 | | | |

**FEBRUARY 2025**

| 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 | |



## Events - India

- IdentityShield Summit, Pune 11-12 Jan
- 4th Edition Cyber Security Excellence Awards, Bengaluru 24 Jan
- Nullcon 2025, Goa 1-2 Mar

## Events - Global

**January 2025**

- BSides Cox's Bazar 2024, Bangladesh 10 Jan
- Global Conference on Cyber Security and Cloud Engineering, Honolulu 10-12 Jan
- Cyber Security for Critical Assets, Dubai 21-22 Jan
- Cybersec Asia 2025, Bangkok 22-23 Jan
- Tampa Cybersecurity Summit, Tampa 24 Jan
- SANS Cyber Threat Intelligence Summit & Training, Alexandria & Virtual 27 Jan-3 Feb
- Annual Government Cyber Security Conference, London 29 Jan
- Dallas Cybersecurity Conference, Dallas & Virtual 30 Jan

**February 2025**

- Cyber Security Training at SANS Cyber Security Central, Virtual 3-8 Feb
- HackCon, Oslo 12-13 Feb
- CruiseCon 2025, Florida 8-13 Feb
- OT Security Sydney, Sydney 11 Feb
- Cyber Security for Critical Assets, Perth 12 Feb
- Cyber Security Training, New Orleans & Virtual 17-22 Feb
- Zero Trust World 2025, Orlando 19-21 Feb
- COSAC APAC 2025, Melbourne 25 Feb

**March 2025**

- Convene: Clearwater 2025, Florida 3-4 Mar
- SunSecCon, Pasadena 6-7 Mar
- Next IT Security, Stockholm 13 Mar
- Los Angeles CyberSecurity Conference 2025, Los Angeles 16 Mar
- Gartner Identity & Access Management Summit, London 24-25 Mar
- SANS DFIR Dallas 2025, Dallas & Virtual 24-29 Mar
- Cybersecurity Summit, South Florida 27 Mar
- BSides 2025, San Diego 29 Mar

QCon LONDON by InfoQ

**MARCH 2025**

| S | M | T | W | T | F | S |
|---|---|---|---|---|---|---|
| 30 | 31 | | | | | 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 |

**April 2025**

- Cybersecurity Summit Boston, Boston 2 Apr
- SecureWorld Charlotte, Charlotte 2 Apr
- QCon London, London 7-11 Apr
- Southeast Cybersecurity Summit, Birmingham 9-10 Apr
- 6th Annual CS4CA APAC Summit, Singapore 16-17 Apr
- UK Cyber Week 2025, London 23-24 Apr
- Toronto Cybersecurity Conference, Toronto & Virtual 24 Apr
- RSA Conference, San Francisco 28 Apr-1 May

**APRIL 2025**

| 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 | | | |

**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

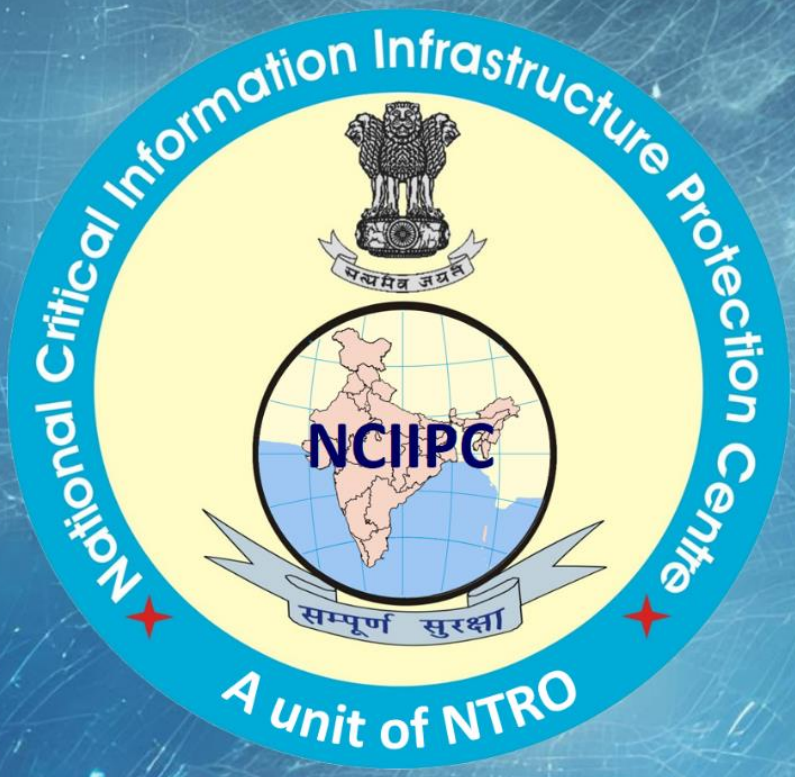
- **AI:** Artificial Intelligence
- **C2:** Command & Control
- **DARPG:** Department of Administrative Reforms and Public Grievances
- **DDoS:** Distributed Denial of Service
- **DoH:** DNS-over-HTTPS
- **FMC:** Firewall Management Center
- **FTD:** Firepower Threat Defense
- **ICCC2024:** International Conference on Cyberlaw, Cybercrime & Cyber Security 2024
- **IoT:** Internet of Things
- **MeitY:** Ministry of Electronics and Information Technology
- **MFA:** Multi-Factor Authentication
- **NCRF:** National Cybersecurity Reference Framework
- **NCX:** National Cyber Exercise
- **RAT:** Remote Access Trojan
- **RRU:** Rashtriya Raksha University
- **SIH:** Smart India Hackathon
- **UDP:** User Datagram Protocol

## Sources


- **Bharat NCX 2024**
  https://pib.gov.in/PressReleasePage.aspx?PRID=2079609
- **GitHub, Telegram Bots, and ASCII QR Codes Abused in Phishing Attacks**
  https://thehackernews.com/
  https://www.linkcpa.com/
- **Gorilla Botnet Launched Over 300,000 DDoS Attacks**
  https://thehackernews.com/
- **Researchers Uncover Hijack Loader Malware**
  https://thehackernews.com/
- **Malware Campaign Used PureCrypter Loader to Deliver DarkVision RAT**
  https://thehackernews.com/
- **Fake AI Video Generators Infect Windows, macOS with Infostealers**
  https://www.bleepingcomputer.com/
- **Linux Variant of FASTCash Malware Targeted Payment Switches in ATM**
  https://www.bleepingcomputer.com/
  https://eu-images.contentstack.com/
- **Salt Typhoon Hackers Backdoor Telcos with GhostSpider Malware**
  https://www.bleepingcomputer.com/
- **Researchers Discover first UEFI Bootkit Malware for Linux**
  https://www.bleepingcomputer.com/
- **Palo Alto Networks Devices Hacked**
  https://thehackernews.com/
- **Google's AI-Powered Tool Discovered Vulnerabilities in OpenSSL**
  https://thehackernews.com/
- **Critical Vulnerability in Microsoft Azure CycleCloud**
  https://msrc.microsoft.com/
  https://nvd.nist.gov/vuln/detail/cve-2024-43602
- **Critical Vulnerability in Siemens Products**
  https://nvd.nist.gov/vuln/detail/CVE-2024-46888
  https://cert-portal.siemens.com/productcert/html/ssa-915275.html,
  https://nvd.nist.gov/vuln/detail/CVE-2024-47553
  https://cert-portal.siemens.com/productcert/html/ssa-430425.html
- **Critical Vulnerability in WordPress AR**
  https://nvd.nist.gov/vuln/detail/CVE-2024-50496
- **Critical Vulnerability in Cisco**
  https://sec.cloudapps.cisco.com/
- **Critical Vulnerability in Camaleon CMS**
  https://nvd.nist.gov/vuln/detail/CVE-2024-46986
- **Critical Vulnerability in macOS**
  https://support.apple.com/en-us/121238,
  https://nvd.nist.gov/vuln/detail/CVE-2024-44148
- **Critical Vulnerability in FreeBSD**
  https://www.freebsd.org/
  https://nvd.nist.gov/vuln/detail/cve-2024-43102

- **First Cyber Policy Dialogue between India and Singapore**
  https://www.mea.gov.in/
- **MeitY Call for Project Proposals in Cyber Security**
  https://www.meity.gov.in/
- **Australia to Mandate Reporting of Ransomware Payments**
  https://oia.pmc.gov.au/
  https://therecord.media/
- **Free ISP Data Breach Exposed Personal Information**
  https://www.darkreading.com/
- **Google Cloud to Require Multi-Factor Authentication by 2025**
  https://www.bleepingcomputer.com/
- **PSAUX Ransomware Targets Over 22,000 CyberPanel Servers**
  https://www.bleepingcomputer.com/
- **Cybersecurity Firm Defends Against Record-Breaking 3.8 Tbps DDoS Attack Targeting Critical Sectors**
  https://thehackernews.com/
- **Mobile and IoT Cyber Threats on the Rise**
  https://www.zscaler.com/
- **Google Stopped Sideloading of Unsafe Android Apps**
  https://thehackernews.com/
- **TrickMo Banking Trojan Evolves: StealsAndroid PINs and Unlock Patterns**
  https://thehackernews.com/
- **SpyLoan: A Global Cyber Threat Fueled by Social Engineering**
  https://www.mcafee.com/
- **Benefits of AI in Cybersecurity**
  https://secureframe.com/blog/ai-in-cybersecurity

# Notes




**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.