NEWSLETTER

January 2024

National Critical Information Infrastructure Protection Centre

(A unit of National Technical Research Organisation)

SECURING WIRELESS NETWORKS

- Enable WPA3/WPA2 with AES Encryption
- Change Router's Default Password
- Disable Unnecessary Services
- Disable SSID Broadcasting
- Disable Wi-Fi/Bluetooth/NFC when not in use
- Enforce Access Control through MAC Address Filtering
- Implement Network Segmentation for Enhanced Isolation
- Keep Router Firmware up-to-date
- Configure Guest Network Wi-Fi for Visitor(s)
- Do Not Share Sensitive Data over Public Wi-Fi/Bluetooth/NFC
- Conduct Security Audits to Mitigate Vulnerabilities
- Aware Users About Potential Risks & Best Security Practices

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

VOLUME 8 ISSUE 1

@NCIIPC

NCIIPC Newsletter

January 2024

Inside This Issue

Message from the NCIIPC Desk

Dear Readers,

It was the 16th January 2014 when Government of India declared formation of National Critical Information Infrastructure Protection Centre (NCIIPC) via a Gazette Notification. In the first decade of its formation, NCIIPC has persued the identification and protection of Critical Information Infrastructure (CII). It has been working in collaboration with various Central Governments, Ministries, Regulators, Institutions, State Government and Private Bodies etc. for identification and declaration of Protected Systems. NCIIPC has identified 7 critical sectors Telecom, Transport, Power & Energy, Banking Financial Services & Insurance, Strategic & Public Enterprises, Government and Health.

During the last quarter of 2023, NCIIPC conducted various workshops and awareness programs for all Critical Sector stakeholders. A workshop on Cybersecurity Capability Maturity Model was organised in collaboration with C3iHub, IIT Kanpur. Various Cybersecurity awareness programs were conducted for each critical sector during National Cyber Security Awareness Month. Cyber Security Awareness Quiz was conducted in the month of October 2023 to help critical sector organisations assess the Cyber Security Awareness of their employees.

Please share the feedback/suggestion on newsletter[at]nciipc[dot]gov[dot]in. The selected feedback/suggestions will also be published.

News Snippets - National

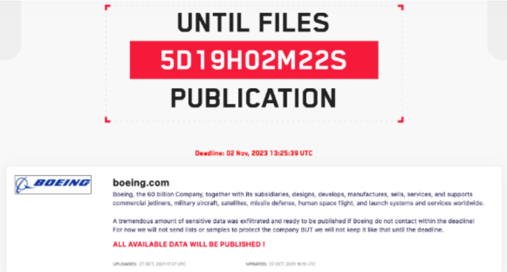
The Union Cabinet to Approve India AI Programme Soon

The Union Minister of State for Electronics and Information Technology, Sh. Rajeev Chandrasekhar stated that the Government of India aims to secure its own digital workspace and digital footprint which would lead to a significant expansion of the market for these technologies, products, and platforms in the coming months. The minister acknowledged the lack of awareness about cybersecurity, even among Chief Information Security Officers (CISOs), and proposed revamp by conducting the Information Security Awareness programme and creating a recurrent training schedule every year. Sh. Chandrasekhar also confirmed that 'India AI programme' will soon be approved by the cabinet. A large Indian dataset programme is said to be developed providing curated access to datasets for the Indian research ecosystem, government, and startup ecosystem. The plan is to mandate any private platform anonymising personal data for their models to also mirror in the government's anonymised data repository. Sh. Chandrasekhar encouraged startups to thrive and innovate in AI within the boundaries to maintain safety and personal accountability measures.

News Snippets - International

LockBit Ransomware Exposes Gigabytes of Boeing Data

The LockBit ransomware gang has publicly released data stolen from Boeing, a major aerospace company, after the company allegedly ignored warnings about the data's impending publication. Prior to the leak, the hackers threatened to release a sample of approximately 4GB of recent files. On November 10, LockBit carried out its threat, making public all the data it had obtained from Boeing, totaling over 43GB. The leaked files include configuration backups for IT management software, as well as logs for monitoring and auditing tools. Although Boeing confirmed the cyberattack, the company has not disclosed specific details about the incident or how the hackers gained access to its network.



UNTIL FILES
5D19H02M22S
PUBLICATION

Deadline: 02 Nov, 2023 13:25:39 UTC

BOEING

boeing.com

Boeing, the 60 billion Company, together with its subsidiaries, designs, develops, manufactures, sells, services, and supports commercial jetliners, military aircraft, satellites, missile defense, human space flight, and launch systems and services worldwide.

A tremendous amount of sensitive data was exfiltrated and ready to be published if Boeing do not contact within the deadline! For now we will not send lists or samples to protect the company BUT we will not keep it like that until the deadline.

ALL AVAILABLE DATA WILL BE PUBLISHED !

UPLOADED: 27 OCT, 2023 17:27 UTC UPDATED: 27 OCT, 2023 18:19 UTC

Boeing page on LockBit data leak site

Okta's Customer Support Data Breach Impacted Customers

Identity and authentication management provider Okta has disclosed that the recent breach in its support case management system impacted 134 out of its 18,400 customers. An unauthorised access occurred between September 28 and October 17, 2023, allowing the intruder to obtain HAR (HTTP Archive) files containing session tokens, subsequently used for session hijacking attacks. Okta's Chief Security Officer, David

Intruder to obtain HAR (HTTP Archive) files containing session tokens, subsequently used for session hijacking attacks.

**Please refer page 21 & 22 for reference.*

Bradbury, revealed that the threat actor successfully hijacked the legitimate Okta sessions of five customers, including 1Password, BeyondTrust, and Cloudflare. Investigations found that the breach exploited a service account within Okta's customer support system, whose credentials were stored in an employee's personal Google account. Okta has taken corrective measures by revoking compromised session tokens, disabling the compromised service account, and blocking the use of personal Google profiles on Okta-managed laptops. Additionally, Okta has introduced session token binding based on network location as a security enhancement. This incident follows Okta's recent revelation of a breach involving personal information of 4,961 current and former employees, exposed through its healthcare coverage vendor, Rightway Healthcare, on September 23, 2023. The compromised data included names, Social Security numbers, and health or medical insurance plans.

Credentials were stored in an employee's personal Google account.

DP World cyberattack Blocks Thousands of Containers in Ports

A devastating cyberattack on DP World Australia, a major international logistics firm, has led to significant disruptions in freight movements across several large Australian ports. DP World specialises in cargo logistics, port terminal operations, maritime services, and free trade zones, operating in 40 countries with 82 terminals. The cyberattack, which occurred on November 10, severely impacted landside freight operations at DP World's ports, prompting the activation of emergency plans and engagement with cybersecurity experts to address the aftermath. Approximately 30,000 shipping containers, containing time-sensitive goods such as blood plasma, wagyu beef, and lobsters, have remained stranded since the attack. The damages are estimated to be in the millions of dollars. While the possibility of data access and exfiltration has been mentioned, an internal investigation was initiated.

Approximately 30,000 shipping containers, containing time-sensitive goods such as blood plasma, wagyu beef, and lobsters, have remained stranded since the attack.

Hackers Breach Healthcare Organisations

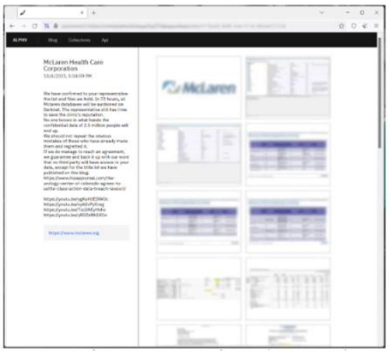
A series of cyberattacks targeting multiple healthcare organisations in the U.S. Exploiting the ScreenConnect remote access tool, threat actors have utilised local ScreenConnect instances associated with Transaction Data Systems (TDS), a nationwide provider of pharmacy supply chain and management systems. The attacks, identified by managed security platform Huntress, occurred between October 28 and November 8, 2023. The compromised endpoints, operating on a Windows Server 2019 system, belonged to distinct organisations within the pharmaceutical and healthcare sectors, linked by their use of ScreenConnect. The ScreenConnect instance in question is associated with the domain 'rs.tdsclinical[.]com,'

The compromised endpoints, operating on a Windows Server 2019 system, belonged to distinct organisations within the pharmaceutical and healthcare sectors, linked by their use of ScreenConnect.

**Please refer page 21 & 22 for reference.*

tied to TDS. The attacker gained access via an unmanaged on-prem instance that wasn't updated since 2019.

McLaren Health Care, a non-profit healthcare system, had notified approximately 2.2 million individuals about a data breach that occurred between late July and August of 2023. McLaren Health Care detected the security breach on August 22, 2023. Following investigations with external cybersecurity experts, McLaren found that the breach had compromised its systems since July 28, 2023. The exposed data varies for each affected individual, depending on the information shared with McLaren and the services received. The organisation has taken proactive steps by notifying U.S. authorities and impacted individuals, who will receive instructions on enrolling in identity protection services for 12 months. Notably, the ALPHV/BlackCat ransomware group claimed responsibility for an attack on McLaren's network on October 4, threatening to auction the allegedly stolen data set affecting 2.5 million people.



McLaren Health Care Corporation
10/4/2023, 5:04:09 PM

We have confirmed to your representative the list and files we hold. In 72 hours, all Mclaren databases will be auctioned on Darknet. The representative still has time to save the clinic's reputation.
No one knows in what hands the confidential data of 2.5 million people will end up.
We should not repeat the obvious mistakes of those who have already made them and regretted it.
If we do manage to reach an agreement, we guarantee and back it up with our word that no third party will have access to your data, except for the little bit we have published on this blog.
https://www.hipaajournal.com/the-urology-center-of-colorado-agrees-to-settle-class-action-data-breach-lawsuit/

[illegible]

https://www.mclaren.org

McLaren claimed by BlackCat ransomware in October

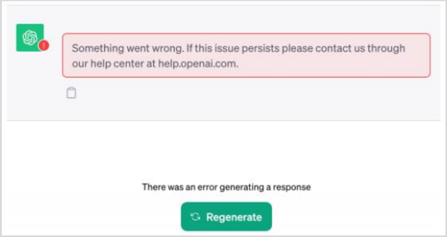
ICBC Confirms Ransomware Attack

The Industrial & Commercial Bank of China (ICBC) has confirmed falling victim to a ransomware attack that disrupted its financial services systems on November 8, 2023 impacting the U.S. treasury market. In response to the incident, ICBC disconnected and isolated affected systems to contain the attack. The bank is conducting investigation and has reported the incident to law enforcement. ICBC emphasised that its business and email systems operate independently from the ICBC Group, and the incident did not affect the systems of ICBC New York Branch, ICBC Head Office, or other affiliated institutions globally. The ransomware attack caused issues in the equities clearing process, prompting the suspension of inbound FIX connections. ICBC's inability to settle U.S. Treasury trades for other market participants resulted in concerns within the financial sector.

The ransomware attack caused issues in the equities clearing process, prompting the suspension of inbound FIX connections.

DDoS Attacks Behind Ongoing ChatGPT Outages

OpenAI addressed periodic outages due to distributed denial-of-service (DDoS) attacks targeting its API and ChatGPT services. The company confirmed the abnormal traffic pattern indicative of a DDoS attack. Users affected by these issues have encountered error messages such as "Something seems to have gone wrong" and "There was an error generating a response." This followed a series of incidents, including a major outage affecting ChatGPT and its API, partial outages, and elevated error rates for Dall-E (an AI system). The incident was resolved and status of services have returned to normal on 09 November 2023.



Something went wrong. If this issue persists please contact us through our help center at help.openai.com.

There was an error generating a response

ChatGPT outage

**Please refer page 21 & 22 for reference.*

German Financial Regulator Website Hit by DDoS Attack

The German Federal Financial Supervisory Authority (BaFin) faced a significant challenge as it was grappling with an ongoing distributed Denial-of-Service (DDoS) attack that crippled its website on 1st September 2023. BaFin, responsible for overseeing thousands of financial institutions, including banks, financial, and insurance service providers, is a crucial regulatory body known for imposing substantial fines on major financial entities for various violations. In response to the cyberattack, BaFin has implemented stringent security measures to safeguard its operations, including temporarily taking its public website, "bafin.de," offline. While the organisation reassured the public that essential systems remain unaffected, the website outage disrupted access to crucial consumer information, regulatory measures, and documentation related to investigations.

> *In response to the cyberattack, BaFin has implemented stringent security measures to safeguard its operations.*

Malware Bytes

'MalDoc in PDF' Allows Attackers to Evade Antivirus

A novel antivirus evasion technique called MalDoc in PDF has been identified by cybersecurity researchers. This technique involves creating a file with the characteristics of a PDF, but when opened in Word, it triggers a VBS macro that performs malicious actions. The PDF document embeds a Word document with the VBS macro, configured to download and install an MSI malware file if opened as a .DOC file in Microsoft Office. An associated campaign, particularly targeting Microsoft credentials, has seen a staggering increase of over 2,400 percent since May 2023. This discovery highlights the evolving and sophisticated nature of cyber threats, emphasising the need for constant vigilance and updated security measures.

> *The PDF document embeds a Word document with the VBS macro, configured to download and install an MSI malware file if opened as a .DOC file in Microsoft Office.*

Targeted Phishing Campaign Unveils SuperBear Trojan

A phishing attack, likely aimed at civil society groups in South Korea, has revealed a new remote access trojan (RAT) named SuperBear. The attack targeted a specific activist who received a malicious LNK file from an email impersonating a member of the non-profit organisation Interlabs. When executed, the LNK file triggers a PowerShell command to run a Visual Basic script that fetches additional payloads from a compromised WordPress website. The payloads include the Autoit3.exe binary (solmir.pdb) and an AutoIt script (solmir_1.pdb). The AutoIt script utilises a process injection technique called process hollowing, where malicious code is inserted into a suspended process. An

> *The AutoIt script utilises a process injection technique called process hollowing, where malicious code is inserted into a suspended process. An instance of Explorer.exe is created for this purpose.*

**Please refer page 21 & 22 for reference.*

instance of Explorer.exe is created for this purpose. The injected code introduces a previously unseen RAT named SuperBear that establishes communication with a remote server. SuperBear is designed to exfiltrate data, download and execute additional shell commands, as well as dynamic-link libraries (DLLs). This sophisticated attack underscores the importance of vigilance against targeted phishing and the need for robust cybersecurity measures to detect and mitigate such threats. It is recommended to never click on any links or attachments in an email unless it is certain that it's safe.

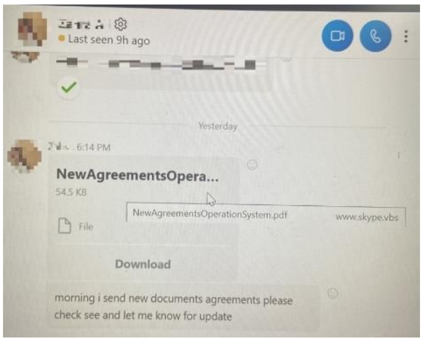
Malicious NuGet Package Targets .NET Developers

A malicious NuGet package within the .NET Framework, named *Pathoschild.Stardew.Mod.Build.Config,* has been discovered delivering the SeroXen RAT in a targeted attack on developers. This package is a deliberate misspelling (typosquat) of the legitimate *Pathoschild.Stardew.ModBuildConfig.* The attack involves a script, tools/init.ps1, executed during package installation to achieve code execution discreetly. The tools/init.ps1 script downloads an obfuscated Windows Batch file (x.bin) from a remote server, responsible for constructing and executing another PowerShell script to deploy the fileless SeroXen RAT. SeroXen RAT combines features from Quasar RAT, the r77 rootkit, and NirCmd, posing a significant threat. Exploiting developers' trust, the attacker injects malicious code into a reputable codebase, specifically targeting cloud credentials exfiltration. Additionally, the campaign includes a deceptive package, telethon2, mimicking the legitimate telethon Python library to interact with Telegram's API, with the intention of targeting Telegram.

The tools/init.ps1 script downloads an obfuscated Windows Batch file (x.bin) from a remote server, responsible for constructing and executing another PowerShell script to deploy the fileless SeroXen RAT.

Messaging Services Infected with DarkGate Malware

DarkGate malware has been observed spreading through instant messaging platforms like Skype and Microsoft Teams. In these incidents, attackers utilised these messaging apps to distribute a Visual Basic for Applications (VBA) loader script camouflaged as a PDF file. Upon opening, the script initiates the download and execution of an AutoIt script, facilitating the launch of the DarkGate malware. The threat actor exploited a trusted relationship between organisations, deceiving recipients into executing the attached VBA script. By gaining access to the victim's Skype account, the attacker took control of an existing messaging thread and manipulated file naming conventions to align with the context of the chat history. The VBA script acted as a conduit to fetch the legitimate AutoIt application (AutoIt3.exe) and an associated AutoIT script, responsible for initiating the DarkGate malware. In an alternative attack scenario, the threat actors sent a Microsoft Teams message containing a ZIP archive



[redacted]
Last seen 9h ago

[redacted]

Yesterday

6:14 PM

NewAgreementsOpera...
54.5 KB
File
NewAgreementsOperationSystem.pdf www.skype.vbs
Download

morning i send new documents agreements please check see and let me know for update

Skype message with an embedded malicious attachment posing as a PDF file

*Please refer page 21 & 22 for reference.

attachment. This archive carries an LNK file, which runs a VBA script. The VBA script is crafted to fetch AutoIt3.exe and the DarkGate artifact.

StripedFly Malware Infected 1 Million Devices

A malware named StripedFly, posing as a cryptocurrency miner, has evaded detection for over five years, infecting over one million devices globally. The malicious shellcode, delivered through an exploit, is capable of downloading binary files from a remote Bitbucket repository and executing PowerShell scripts. It supports expandable features for data harvesting, self-uninstallation, and operates as a monolithic binary with modular capabilities. The malware utilises a built-in TOR network tunnel for communication with command servers and leverages trusted services like GitLab, GitHub, and Bitbucket for updates and delivery, employing custom encrypted archives. Once established, the malware disables the SMBv1 protocol and spreads to other machines via a worming module using both SMB and SSH, utilising harvested keys. Persistence of StripedFly is achieved through modifications to the Windows Registry or the creation of task scheduler entries, especially when administrative access is available and the PowerShell interpreter is installed.

The malicious shellcode, delivered through an exploit, is capable of downloading binary files from a remote Bitbucket repository and executing PowerShell scripts.

Hackers Launch Malware Attacks Tech Sector

Imperial Kitten, a threat actor group, has launched a new campaign targeting transportation, logistics, and technology companies. CrowdStrike, a cybersecurity firm, has identified phishing attacks within this campaign, featuring emails themed as 'job recruitment' and carrying a malicious Microsoft Excel attachment. Upon opening the document, a malicious macro code extracts two batch files, enabling persistence through registry modifications and executing Python payloads for reverse shell access. The attacker then progresses laterally on the network, utilising tools like PAExec for remote process execution, NetScan for network reconnaissance, and ProcDump to extract credentials from system memory. Communication with the command and control (C2) server is established through custom malware, IMAPLoader and StandardKeyboard, both relying on email as a means of information exchange.

Upon opening the document, a malicious macro code extracts two batch files, enabling persistence through registry modifications and executing Python payloads for reverse shell access.

Massive Akira Ransomware Attack Thwarted

Akira ransomware actors targeted an industrial organisation in June 2023. The attack utilised devices not integrated with Defender for Endpoint, employed defence evasion tactics, and involved reconnaissance and lateral movement activities before encrypting devices with a compromised user account. The automatic attack disruption feature of Microsoft Defender

*Please refer page 21 & 22 for reference.

contained the breach by restricting the compromised accounts from accessing endpoints and other network resources, limiting the attackers' lateral movement capabilities irrespective of the account's Active Directory status or privilege level.

Threat Actor Exploited Microsoft SQL Servers

A campaign named DB#JAMMER was identified, where threat actors exploited insecure Microsoft SQL (MSSQL) servers to deploy Cobalt Strike and the FreeWorld ransomware. The attack involved brute-forcing MS SQL servers for initial access, used them to enumerate databases, and exploited the xp_cmdshell configuration to run shell commands and performed reconnaissance. Subsequently, the attackers impair the system firewall, establish persistence by connecting to a remote SMB share, transfer files, and install malicious tools like Cobalt Strike. Lateral movement is then conducted before distributing AnyDesk software, ultimately leading to the deployment of the FreeWorld ransomware.

Subsequently, the attackers impair the system firewall, establish persistence by connecting to a remote SMB share, transfer files, and install malicious tools like Cobalt Strike.

Learning

Planning Considerations for Cyber Incidents

The Federal Emergency Management Agency (FEMA) in collaboration with the Cybersecurity and Infrastructure Security Agency (CISA) has released the joint guide intended to help state, local, tribal, and territorial (SLTT) emergency management personnel by providing considerations to prepare for a cyber incident and development of a cyber incident response plan. Incident response plans include response team members and their backups, effective communication between the team members, and the roles of each team member. The plan outlines steps to be taken at each stage of the process and designated team member(s) responsible for each step, as well as emergency managers charged with overall responsibility for the response. With the knowledge and coordination, emergency managers can develop understanding of the cyber risks experienced in their jurisdictions and their potential impacts and thereby increase the community’s preparedness and overall resilience towards a cyber incident. Key aspects in preparing for cyber incident include:

- Understanding all types of cyber incidents that may occur
- Engaging service owners and operators
- Determining critical services and related dependencies
- Prioritising and planning for service and system disruptions
- Clearly identifying roles and responsibilities
- Providing integrated communication and public messaging

The plan outlines steps to be taken at each stage of the process and designated team member(s) responsible for each step, as well as emergency managers charged with overall responsibility for the response.

**Please refer page 21 & 22 for reference.*

Trends

CISA Released Roadmap for Artificial Intelligence Adoption

CISA ROADMAP FOR ARTIFICIAL INTELLIGENCE

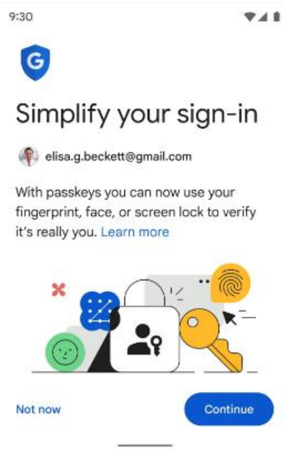
Cybersecurity and Infrastructure Security Agency (CISA) has released a guide for their AI-related efforts, ensuring both internal coherence as well as alignment with the whole-of-government AI strategy. The roadmap incorporates key actions lead by CISA to promote constructive uses of AI, protect AI systems from cybersecurity threats and prevent malicious attackers from using AI to threaten critical infrastructure. The roadmap represents CISA's AI efforts along five lines of effort (LOE):

- Responsibly use AI: CISA will ensure responsible, ethical, and safe use of AI.
- Assure AI systems: CISA will assess and assist secure AI-based software adoption to various stakeholders.
- Protect and support critical infrastructure from malicious use of AI: CISA will assess and recommend mitigation of AI threats faced by critical infrastructures.
- Coordinate and communicate on key AI uses with the interagency, international partners, and the public: CISA will develop DHS-led and interagency processes on AI-enabled software and coordinate with international partners to advance global AI security.
- Expand AI expertise in the workforce: CISA will continue to educate the workforce on AI software systems and techniques along with the legal, ethical, and policy aspects of AI-based software systems.

The roadmap incorporates key actions lead by CISA to promote constructive uses of AI, protect AI systems from cybersecurity threats and prevent malicious attackers from using AI to threaten critical infrastructure.

Google's Innovative Passkeys Set to Revolutionise Sign-Ins

Google announced the ability to set up passkeys by default, supported by the FIDO Alliance. Passkeys are a new form of passwordless login mechanism that uses public-key cryptography to authenticate a users' access to any website or app, where the private key and public key are saved securely in the device and the server respectively. Each passkey is unique and synced to a username and a specific service, which means, a user has at least as many passkeys as they have accounts. Therefore, when a user signs into a website or app with passkey mechanism, a random challenge is created and sent to the client, which prompts user to verify using biometric or PIN to sign the challenge using the private key and send back to the server. If the signed response can be validated using the associated public key, authentication is considered successful. Benefits of passkeys includes avoiding the hassle of remembering passwords and they are phishing-resistant, hence safeguarding accounts against potential takeover attacks. Microsoft has officially began supporting passkeys in Windows 11 and platforms like eBay and Uber have also enabled passkeys for improved account security.



9:30

Simplify your sign-in

elisa.g.beckett@gmail.com

With passkeys you can now use your fingerprint, face, or screen lock to verify it's really you. Learn more

Passkeys Notification

Please refer page 21 & 22 for reference.

Vulnerability Watch

Apache ActiveMQ Vulnerability in Hitachi Energy

Critical Remote Code Execution vulnerability discovered in Apache ActiveMQ affects Hitachi Energy's SOI (Service Oriented Integration) product. This vulnerability having CVE ID CVE-2023-46604 and CVSS score 10.0 can be exploited to do remote code execution that can be used to carry out various types of attacks. The affected versions are SOI versions 2.0.0 to 2.2.0. It is recommended to apply the patch SOI EP1a and follow the general mitigation factors/workarounds to ensure that proper firewall protection and detection/monitoring are implemented.

This vulnerability having CVE ID CVE-2023-46604 and CVSS score 10.0 can be exploited to do remote code execution that can be used to carry out various types of attacks.

Vulnerability in XXL-RPC

Critical Deserialisation of Untrusted Data vulnerability has been discovered in XXL-RPC, a distributed RPC framework. When a TCP server is set up using the Netty framework and the Hessian serialisation mechanism it is vulnerable to this vulnerability having CVE ID CVE-2023-45146 with CVSS score 10.0. An attacker can execute arbitrary code and take control of the server machine by providing malicious serialised objects.

An attacker can execute arbitrary code and take control of the server machine by providing malicious serialised objects.

Multiple Vulnerabilities in Cisco IOS XE Software

A critical vulnerability having CVE ID CVE-2023-20198 and CVSS score 10.0 has been discovered in the web UI feature of Cisco IOS XE Software. When exploited this vulnerability allows an attacker to gain initial access and issue a privilege 15 command to create a local user and password combination, thereby allowing attacker to log-in with normal user access. The attacker also exploited another component of the web UI feature by manipulating the newly created local user to elevate privilege to root and write the implant to the file system. This vulnerability has CVE ID CVE-2023-20273 and CVSS score 7.2. Cisco has released security updates to address these vulnerabilities.

Critical Vulnerabilities in macOS Sonoma

A permission vulnerability having CVE ID CVE-2023-40455 and CVSS score 10.0 has been discovered in macOS Sonoma (the latest release of macOS). Similarly, an access vulnerability was addressed with additional sandbox restrictions in macOS Sonoma. This vulnerability has CVE ID CVE-2023-38586 and CVSS score 10.0. These vulnerabilities have been fixed in macOS Sonoma 14.

Vulnerability in TinyLab

Critical insecure permissions vulnerability having CVE ID CVE-2022-42150 with CVSS score 10.0 has been discovered in TinyLab linux-

*Please refer page 21 & 22 for reference.

lab and cloud-lab. Tinylab is an open source electronic lab. The affected versions are TinyLab linux-lab v1.1-rc1 and cloud-labv0.8-rc2, v1.1-rc1.

Critical Vulnerability in WireMock

Server-Side Request Forgery (SSRF) vulnerability has been discovered in WireMock, a tool for mocking HTTP services. The vulnerability has CVE ID CVE-2023-39967 with CVSS score 10.0. When certain request URLs are used in WireMock Studio configuration fields, the request could be forwarded to an arbitrary service reachable from WireMock's instance. WireMock has discontinued the affected Wiremock studio product and there will be no fix.

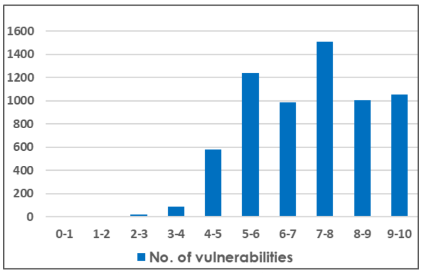
Multiple Vulnerabilities in Zephyr

Zephyr is a small real-time operating system for resource-constrained, connected and embedded devices. An off-by-one buffer overflow vulnerability has been discovered in the Zephyr fuse file system. This vulnerability has CVE ID CVE-2023-4260 having CVSS score 10.0. Similarly, buffer overflow vulnerability has been discovered in Zephyr mgmt subsystem. This vulnerability has CVE ID CVE-2023-4262 having CVSS score 10.0.

Quarterly Vulnerability Analysis Report

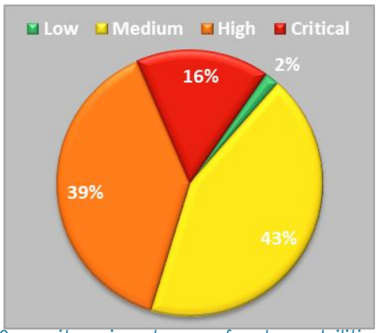
Knowledge Management Team, NCIIPC

During the last quarter of 2023, a total of 6492 vulnerabilities have been observed, out of which majority of vulnerabilities have score ranging from 4-7. 16 percent of total vulnerabilities reported were of Critical severity. Microsoft, Google, Apple, Fedoraproject and Linux were the top five vendors having 21 percent of total reported vulnerabilities.



Severity-wise number of vulnerabilities

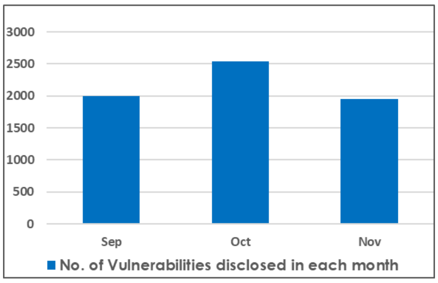
Severity	CVSSv3 Score	Number of Vulnerabilities			Total Vulnerabilities	Severity Total
		Sep'23	Oct'23	Nov'23		
Low	0-1	0	0	6	6	116
	1-2	0	0	0	0	
	2-3	5	11	3	19	
	3-4	39	29	23	91	
Medium	4-5	193	230	158	581	2807
	5-6	405	470	366	1241	
	6-7	307	363	315	985	
High	7-8	465	606	440	1511	2515
	8-9	237	421	346	1004	
Critical	9-10	351	414	289	1054	1054
Total		2002	2544	1946		6492



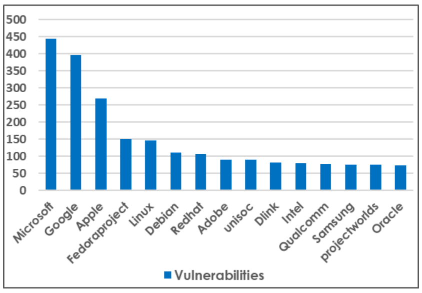
Severity-wise share of vulnerabilities

**Please refer page 21 & 22 for reference.*

S. No.	Vendor	No. of Vulnerabilities			Total
		Sep'23	Oct'23	Nov'23	
1.	Microsoft	107	145	191	443
2.	Google	135	197	64	396
3.	Apple	132	66	71	269
4.	Fedoraproject	60	45	46	151
5.	Linux	60	50	36	146
6.	Debian	46	39	26	111
7.	Redhat	31	36	39	106
8.	Adobe	8	12	70	90
9.	unisoc	40	24	26	90
10.	Dlink	48	33	0	81
11.	Intel	1	0	78	79
12.	Qualcomm	32	22	23	77
13.	Samsung	32	11	33	76
14.	projectworlds	15	13	48	76
15.	Oracle	1	73	0	74



No. of vulnerabilities disclosed in each month



Count of vulnerabilities for top 15 vendors

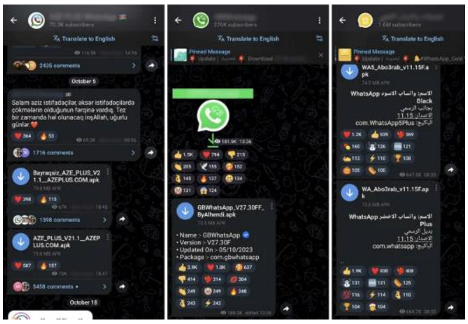
Mobile Security

PEACHPIT: Massive Ad Fraud Botnet

Cybersecurity researchers from HUMAN have recently discovered an ad fraud botnet named PEACHPIT which has affected thousands of Android and iPhone devices to generate illicit profits. This botnet is a part of an operation codenamed BADBOX which is found to be running huge ad frauds over 220 countries. The infection has been carried out with 39 apps that were installed more than 15 million times. Devices infected with BADBOX allowed malicious users to create residential proxy exit peers, steal sensitive data and commit ad fraud. It was observed that the Android and iOS devices were compromised through backdoors created using malicious firmware which can also compromise one-time passwords for apps such as Gmail and WhatsApp.

Modified WhatsApp Versions Infected with CanesSpy Spyware

Cybersecurity researchers have identified modified version of WhatsApp for Android which comes with spyware module named CanesSpy. Such modified applications have been observed propagated through websites advertising as well as Telegram channels used primarily by Arabic and Azerbaijani speakers. Once infected, it establishes connection with a command-and-control (C2) server and sends all the information such as phone number, IMEI, mobile country code, mobile network code and transmits details about the victim's accounts and contacts in every five minutes. CanesSpy spyware has been active since mid of August 2023, primarily targeting Azerbaijan, Saudi Arabia, Turkey, Yemen, and Egypt.


Translate to English

2435 comments

October 5

Salam aziz istifadəçilər, aksər istifadəçilərdə çökmələrin olduğunun fərqinə vardıq. Tez bir zamanda həl olunacaq inşAllah, uğurlu günlər.❤️

1716 comments

Bayraqsiz_AZE_PLUS_V21.1__AZEPLUS.COM.apk

1398 comments

AZE_PLUS_V21.1__AZEPLUS.COM.apk

5458 comments

October 18

Translate to English

Pinned Message

GBWhatsApp_V27.30FF_ByAlhendi.apk

- Name :- GBWhatsApp
- Version :- V27.30F
- Updated On :- 05/10/2023
- Package :- com.gbwhatsapp

Translate to English

Pinned Message

WA5_Abo3rab_v11.15F.apk

الاسم: واتساب الاسود WhatsApp Black
بجانب الرسمي
الاصدار: 11.15
الباكيج: com.WhatsApp5Plus

WA_Abo3rab_v11.15F.apk

الاسم: واتساب الاخضر WhatsApp Plus
بديل الرسمي
الاصدار: 11.15
الباكيج: com.whatsapp

Infected WhatsApp

Please refer page 21 & 22 for reference.

Android Trojan SpyNote Records Audio and Phone Calls

In a recent surge of cyber threats targeting Android users, security experts have identified a potent Trojan named SpyNote, capable of recording audio and phone calls without the device owner's knowledge. The discovery raises concern about user privacy and the increasing sophistication of malware targeting mobile devices. The Trojan typically spreads through malicious apps disguised as legitimate applications, often infiltrating third party app stores or through deceptive links. SpyNote's capabilities extend beyond eavesdropping, as it can also gain access to text messages, location data, and other sensitive information stored on the infected device. The Trojan's covert operation poses a significant threat to user privacy and raises questions about the effectiveness of current security measures in the Android ecosystem. As the cyber security community works to develop countermeasures against SpyNote and similar threats, users are encouraged to stay vigilant and adopt proactive security practices to safeguard their personal information. In an era where digital privacy is paramount, the battle against sophisticated malware underscores the need for continuous efforts to protect the integrity of mobile devices.

> *SpyNote's capabilities extend beyond eavesdropping, as it can also gain access to text messages, location data, and other sensitive information stored on the infected device.*

NCIIPC Initiatives

NCIIPC at Power Sector Cyber Security Conference 2023

The Cyber Security Association of India organised 'Power Sector Cyber Security Conference 2023' on 19th December 2023 at New Delhi. This conference aims to enhance cybersecurity measures for the foundational components of our national critical information infrastructure – the Power Sector. The conference featured a session delivered by Sh. Navin Kumar Singh, DG NCIIPC focusing on SOC effectiveness, ISO 27001, ISO 27019, Risk based framework, Cyber Security manpower, People Process Tech, Audit and Risk management, IOT, Smart Grid and Smart Meter Threats.

Sh. Navin Kumar Singh,DG NCIIPC at Power Sector Cyber Security Conference

NCIIPC at Cybersecurity Capability Maturity Model Workshop

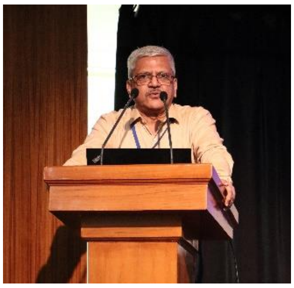
NCIIPC organised 1st Workshop on Cybersecurity Capability Maturity Model (CSCMM) Development, in collaboration with C3iHub, IIT Kanpur on 3rd & 4th November 2023. The workshop was inaugurated by Sh. Navin Kumar Singh, DG NCIIPC. Mr. Cliff Glantz and Dr. Shuchismita Biswas from the Pacific Northwest National Laboratory (PNNL), United States, shared their insights on the C2M2 model, developed by PNNL, added immense value to the discussions on cybersecurity capabilities. CISOs of various public and private organisations like HDFC, LIC, ICICI attended the workshop.

Sh. Navin Kumar Singh,DG NCIIPC at Cybersecurity Capability Maturity Model Workshop

*Please refer page 21 & 22 for reference.

NCIIPC at 'Cyber Security - Importance & Challenges'

The National Power Training Institute (NPTI) observed National Cyber Security Awareness Month (NCSAM) 2023/Cyber Jagrookta Diwas (CJD) by hosting a one-day National Seminar on 'Cyber Security — Importance & Challenges' on 31st October 2023 at R&I Park, IIT Delhi. The event featured a session delivered by Sh. K. Pradeep Bhat, Consultant NCIIPC, focusing on Cyber Security workforce development for Critical Sector Entities.



Sh. K. Pradeep Bhat, Consultant NCIIPC at IIT Delhi

NCIIPC Organised Cyber Security Awareness Program

NCIIPC organised Cyber Security Awareness Program with theme as “Secure Our World” and other important threads relevant for cyber security in Critical Sectors as a part of the “National Cyber Security Awareness (NCSAM) 2023” campaign for the Critical Sector entities during the month. The programmes covered the cyber security threat landscape in recent times due to ransomware, outsourcing and from state backed actors.

Awareness Program for Strategic and Public Enterprises (S&PE) Sector Organisations was held on 26th October 2023. More than 130 participants from different ministries/organisations under S&PE sector attended the program.

Sh. Lokesh Garg, DDG NCIIPC at Cyber Security Awareness Program for S&PE Sector Organisations

A webinar focusing on Cyber Security Awareness Program for Telecom Sector entities was held on 26th October 2023. 140 participants from various Telecom Sector organisations (DoT, BSNL, MTNL, BBNL, RailTel, POWERTEL, Airtel, JIO and VIL) across the country attended the same.

Awareness program for Power & Energy sector was held on 18th October 2023. More than 330 participants from around 60 organisations participated in this program.

Awareness program in Transport sector was held on 19th October 2023. More than 500 participants from around 20 organisations participated in this awareness program.

Awareness program in BFI Sector was held on 27th October 2023. More than 70 organisations participated in this awareness program. Various themes like Common Weakness in Implementation of Cyber Security Controls, and Effective Internal Cyber Security Audit, etc. were covered during this awareness program.

Awareness program in Government sector held on 30th October 2023. More than 80 participants from more than 20 organisations participated in this awareness program. NCIIPC discussed its role in CII protection and the responsibilities of CISOs.

Awareness program in Health sector held on 30th October 2023. More than 100 participants from more than 25 organisations participated in this awareness program. Many topics like How to

**Please refer page 21 & 22 for reference.*

protect Health Industry from Ransomware and APTs and etc. were discussed in this program.

Awareness program for all Critical Sectors on common themes of relevance was held on 31st October 2023. More than 650 participated in this program. Following themes were covered during the awareness program:

- Cyber Security Threats from MSP and MSSP and way forward.
- Threats from AI and way forward.
- Case Study 1: Insights from IR related to incidents by APT actors.
- Operational aspects of Effective Security Operations Centre (SOC).
- Case Study 2: Insights on recent Malware Trends.
- Importance of having strong in-house cyber security team.
- Importance of Red and Blue Teaming in cyber security.

NCIIPC conducted "Cyber Security Awareness Quiz 2023" as part of the NCSAM 2023 for the employees of all the Critical Sector entities. More than 13000 participants from nearly 200 organisations participated in the quiz.

NCIIPC at Cyber Security Awareness Program for Government of Karnataka

NCIIPC delivered a session on Phishing attacks, Supply Chain and Social Engineering attacks and mitigation techniques during Cyber Security awareness program for Government of Karnataka on 18th October 2023.

NCIIPC at "Cyber Security Complaince-Challenges and Opportunities" Conference

NCIIPC delivered a session on CII Complaince in the conference on "Cyber Security Complaince-Challenges and Opportunities". The conference was organised by Indian Oil Corporation Ltd. (IOCL), on 27th October 2023.

NCIIPC at Cyber Security Awareness Month Program for GAIL

NCIIPC delivered a keynote lecture on Cyber Security at GAIL Corporate office on 30th October 2023 as part of their Cyber Security Awareness Month program.

NCIIPC at "International Conference on Cyberlaw, Cybercrime and Cybersecurity" Conference

NCIIPC participated in "International Conference on Cyberlaw, Cybercrime and Cybersecurity" Conference organised by

*Please refer page 21 & 22 for reference.

Cyberlaws.Net and Pawan Duggal Associates, advocates at Scope Convention Centre, New Delhi.

NCIIPC at One-day Cyber Security Workshop for Power Sector

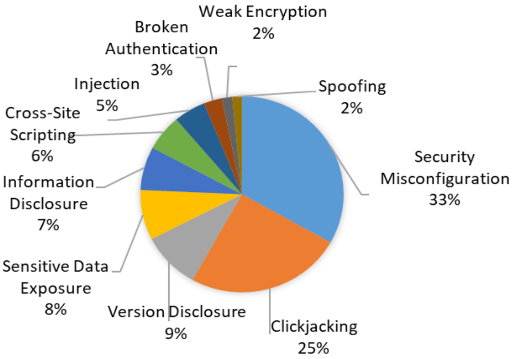
One-day cyber security workshop dedicated to distribution utilities in Power Sector named "Cyber Security Workshop for Distribution utilities in Power Sector" was organised by Central Electricity Authority (CEA) on 15 December 2023 at Rural Electrification Corporation (REC), Gurugram. Sh. Neeraj Saini, Director NCIIPC delivered a session on “Practice Measures for Identified CII in Distribution Sector” in this workshop.

Sh. Neeraj Saini, Director NCIIPC at the workshop

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 2776 vulnerabilities reported during the last quarter of 2023. The top 10 vulnerabilities are:

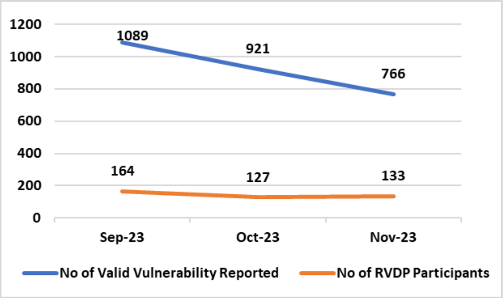
- Security Misconfiguration
- Clickjacking
- Version Disclosure
- Sensitive Data Exposure
- Information Disclosure
- Cross-Site Scripting
- Injection
- Broken Authentication
- Weak Encryption
- Spoofing



Around 424 researchers participated in RVDP programme during the last quarter of 2023. NCIIPC acknowledges following top 15 researchers for their contributions (names are in alphabetical order):

- Abhay Dev Js
- Abhishrey Gupta
- Abishek R
- Affan Ahmed
- Akanksha Verma
- Akhil Subrahmanyan
- Amana Fathima N

**Please refer page 21 & 22 for reference.*



vulnerabilities and RVDP participants

- Anant Deoashish Beck
- Divesh Mandhyan
- Harikrishnan K V
- Hrishikesh Patra
- Ishwar Kumar
- Nikhil Jagtap
- Sharanabasappa Kalyan
- Sreerag A S

**Please refer page 21 & 22 for reference.*

Upcoming Events - Global

intersec 25 YEARS

January 2024

SANS London January 2024, London & Virtual	8-13 Jan
The International Conference on Cyber Security 2024, New York	8-10 Jan
Vision 2024: Looking Ahead at Cyber Threats, Virtual	11 Jan
INTERSEC Dubai 2024, Dubai	16-18 Jan
AI Virtual Cybersecurity Summit, Virtual	25 Jan
IT Security Insights 2024, Stockholm	31 Jan
Cybersec Asia, Bangkok	31 Jan–1 Feb
Ca IT-Defense 2024, Stuttgart	31 Jan-2 Feb

JANUARY 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			

February 2024

CYSEC Qatar Summit 2024, Doha	7 Feb
Phoenix-Scottsdale Cybersecurity Conference, Arizona	8 Feb
CyberForge 2024, Virginia	10-11 Feb
Silicon Valley Cyber Security Summit, Santa Clara	13 Feb
HackCon, Oslo	14-15 Feb
Detroit Cybersecurity Conference, Detroit	15 Feb
2024 Palmetto Cybersecurity Summit, Columbia	21-22 Feb

FEBRUARY 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		

CYBER·SC
Palmetto Cyber Summit 2024
The premier gathering of South Carolina's cybersecurity professionals.
Columbia, South Carolina
February 21-22, 2024

March 2023

Ransomware Resilience Conference 2024, Kuala Lumpur	4-5 Mar
Vancouver International Privacy & Security Summit 2024, Vancouver	6-8 Mar
Austin API Summit 2024, Austin	11-13 Mar
Black Hat Trainings, Washinton	12-15 Mar
Ohio Information Security Conference, Dayton	13 Mar
BSides Transylvania, Transylvania	23 Mar
AISA Australian Cyber Conference, Canberra	25-27 Mar

AUSTRALIAN CYBER CONFERENCE 2024

MARCH 2024

S	M	T	W	T	F	S
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	30

APRIL 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				

April 2024

Cybertech Global Tel Aviv 2024, Tel Aviv	8-10 Apr
Baltimore Cyber Security Summit, Baltimore	4 Apr
Philadelphia Cybersecurity Conference, Philadelphia & Virtual	4 Apr
Nashville Cyber Security Summit, Nashville	5 Apr
SEKOP2024, Hamburg	11-14 Apr
Dallas Cyber Security Summit, Dallas	12 Apr
Qubit Conference Prague 2023, Prague	22-24 Apr
BSides Cymru 2024, Cardiff	27 Apr
National Cyber Security Show 2024, Birmingham	30 Apr-2 May

Upcoming Events - India

International Conference on Cybersecurity and Machine Intelligence, Bhubaneswar	16-17 Jan
Information Security Conclave, Nashik	19-20 Jan
International Conference on Big Data, IoT, Cyber Security and Information Technology, Pune	29 Jan
Gartner Security & Risk Management Summit, Mumbai	26-27 Feb
SANS Secure India, Bengaluru	18–23 Mar

EXPRESS COMPUTER
INFORMATION SECURITY CONCLAVE
ELEVATE, EMPOWER, AND SECURE: THE PROACTIVE ENTERPRISE IMPERATIVE
19 20 JANUARY 2024
RADISSON BLU HOTEL & SPA, NASHIK
Information security Conclave
#InfoSecConclave

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

- AIIMS: All India Institute of Medical Sciences
- C2: Command and Control
- CEA: Central Electricity Authority
- CISA: Cybersecurity and Infrastructure Security Agency
- CISO: Chief Information Security Officers
- CJD: Cyber Jagrookta Diwas
- CSCMM: Cybersecurity Capability Maturity Model
- DDoS: Distributed Denial-of-Service
- FEMA: Federal Emergency Management Agency
- HAR: HTTP Archive
- ICBC: Industrial & Commercial Bank of China
- ICMR: Indian Council of Medical Research
- IOCL: Indian Oil Corporation Ltd.
- LOE: Lines of Effort
- MS SQL: Microsoft SQL
- NCSAM: National Cyber Security Awareness
- NCX: National Cyber Security Exercise
- NPTI: National Power Training Institute
- PNNL: Pacific Northwest National Laboratory
- RAT: Remote Access Trojan
- S&PE: Strategic and Public Enterprises
- SLTT: State, Local, Tribal, and Territorial
- SOC: Security Operations Centre
- SOI: Service Oriented Integration
- SSRF: Server-Side Request Forgery
- TDS: Transaction Data Systems
- VBA: Visual Basic for Applications

Sources

- **The Union Cabinet to Approve India AI Programme Soon**
  https://economictimes.indiatimes.com/
  https://www.meity.gov.in/
- **LockBit Ransomware Exposes Gigabytes of Boeing Data**
  https://www.bleepingcomputer.com/
- **German Financial Regulator Website Hit by DDoS Attack**
  https://www.bleepingcomputer.com/
  https://www.bafin.de/
- Ok**ta's Customer Support Data Breach Impacted Customers**
  https://thehackernews.com/
  https://www.okta.com/
- **DP World cyberattack Blocks Thousands of Containers in Ports**
  https://www.bleepingcomputer.com/
  https://www.dpworld.com/
- **Hackers Breach Healthcare Organisations**
  https://www.bleepingcomputer.com/
- **ICBC Confirms Ransomware Attack**
  https://www.bleepingcomputer.com/
  https://www.icbc-ltd.com/
- **DDoS Attacks Behind Ongoing ChatGPT Outages**
  https://www.bleepingcomputer.com/
  https://status.openai.com/
- **'MalDoc in PDF' Allows Attackers to Evade Antivirus**
  https://socradar.io/
- **Targeted Phishing Campaign Unveils SuperBear Trojan**
  https://thehackernews.com/
- **Malicious NuGet Package Targets .NET Developers**
  https://www.scmagazine.com/
  https://www.nuget.org/packages
- **Messaging Services Infected with DarkGate Malware**
  https://www.trendmicro.com/
- **StripedFly Malware Infected 1 Million Devices**
  https://securityaffairs.com/
- **Hackers Launch Malware Attacks Tech Sector**
  https://www.bleepingcomputer.com/
- **Massive Akira Ransomware Attack Thwarted**
  https://securityaffairs.com/
- **Threat Actor Exploited Microsoft SQL Servers**
  https://www.securonix.com/
- **Planning Considerations for Cyber Incidents**
  https://www.fema.gov/
- **CISA Released Roadmap for Artificial Intelligence Adoption**
  https://www.cisa.gov/
- **Google's Innovative Passkeys Set to Revolutionise Sign-Ins**
  https://thehackernews.com/
- **Apache ActiveMQ Vulnerability in Hitachi Energy**
  https://publisher.hitachienergy.com/

- **Vulnerability in XXL-RPC**
  https://nvd.nist.gov/
  https://security.snyk.io/
- **Multiple Vulnerabilities in Cisco IOS XE Software**
  https://sec.cloudapps.cisco.com
  https://nvd.nist.gov/
- **Vulnerability in TinyLab**
  https://nvd.nist.gov/vuln/detail/CVE-2022-42150
- **Critical Vulnerabilities in macOS Sonoma**
  https://support.apple.com/en-us/HT213940
  https://nvd.nist.gov/
  https://www.apple.com/
- **Critical Vulnerability in WireMock**
  https://nvd.nist.gov/vuln/detail/CVE-2023-39967
  https://github.com/
  https://wiremock.org/start/
- **Multiple Vulnerabilities in Zephyr**
  https://nvd.nist.gov/vuln/detail/CVE-2023-4260
  https://nvd.nist.gov/vuln/detail/CVE-2023-4262
  https://www.zephyrproject.org/
- **PEACHPIT: Massive Ad Fraud Botnet**
  https://www.techradar.com/
- **Modified WhatsApp Versions Infected with CanesSpy Spyware**
  https://www.kaspersky.co.in/
- **Android Trojan SpyNote Records Audio and Phone Calls**
  https://www.zdnet.com/

Notes

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.