**Cyber Security Advisories**

**Date: 19 Apr 2024**

1. **Adv/2024/Mar/035**

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\_Adv2024Mar035.txt attached**

1. **Adv/2024/Mar/036**

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\_Adv2024Mar036.txt attached**

1. **Adv/2024/Mar/037**

It has been reported that attackers are targeting Government personnel using spoofed/compromised email IDs, malicious domains and phishing web pages.  The Spear-phishing email contains a hyperlink. Upon click, it opens a mimic/cloned phishing web page of kavach.mail.gov.in. The IP address and the domain on which phishing page is hosted is malicious and involved in compromising user credentials/propagate malware payload.

**IOCs: IOC\_Adv2024Mar037.txt attached**

1. **Adv/2024/Apr/001**

It has been reported that a threat group known as TA866 (aka Asylum Ambuscade) are deploying multiple stages of custom malware, such as Wasabiseed, Screenshotter, AHK Bot, and Resident backdoor. TA866 is deploying Resident backdoor and Rhadamanthys Stealer on victim machines only after the adversary confirms that the victim’s data is valuable. Resident backdoor is a custom backdoor capable of achieving persistence and deploying secondary payloads.  It creates a scheduled task to run every 10 minutes via a Windows task scheduler. The threat group victims are directed to an initial entry point for a 404 Traffic Distribution System (TDS), either via malspam or malvertising, as a means for initial access.  A TDS is an infrastructure cybercriminals use to monitor and manage malicious traffic, which is typically associated with malware distribution. The 404 TDS leads victims to malicious domains that are typically hosting malware. TA866 also uses several web-based techniques to lure victims into unknowingly downloading malware during normal browsing, such as purchasing Google advertisements and poisoning Search Engine Optimization (SEO) rankings. The threat group delivers an additional malware family, AHK Bot, via MSI files. AHK Bot is a modular malware family that consists of AutoHotKey (AHK) scripts. It uses the AutoHotKey utility to execute the malicious AHK scripts.

TA866 also deployed other malware and post-exploitation tools around the same time frame using Resident backdoor:

1. **Adv/2024/Apr/002**

Presence of malicious IoCs found in Indian Cyberspace related to Sogu/PlugX RAT Malware

**IOCs: IOC\_Adv2024Apr002.txt attached**

1. **Adv/2024/Apr/003**

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\_Adv2024Apr003.txt attached**

1. **Adv/2024/Apr/004**

It has been observed that Stately Taurus aka Mustang Panda, BRONZE PRESIDENT, Red Delta, LuminousMoth, Earth Preta and Camaro Dragon is involved in cyberespionage campaigns. Adversary has created two malware packages. The first package ZIP archive contains two files, the exe and DLL file. The exe is a renamed copy of the signed anti-key logging program. Threat actors have taken advantage of legitimate products for malicious purposes. Upon execution, it sideloads malicious DLL and creates an autorun registry key for persistence. The second package is a screensaver executable for the initial infection which resulted in downloading of malicious code from Command & Control (C2).

**IOCs: IOC\_Adv2024Apr004.txt attached**

1. **Adv/2024/Apr/005**

It has been reported 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. Upon extraction, the archive file contains the Windows executable Crimson Rat Malware file. Upon click, malware executes and performs the following functions:-

Defense Evasion (Modify registry, Impair Defense, Abuse Elevation Control Mechanism, Asynchronous procedure call)

Command and Control (Application layer protocol)

Collection (local data staging)

Privilege Escalation (Abuse Elevation control mechanism)

Discovery (System Information Discovery)

Further, the executable file makes a connection with the Command & Control (C2) server and sends the request continuously to the C2 server for response.

**IOCs: IOC\_Adv2024Apr005.txt attached**

1. **Adv/2024/Apr/006**

Presence of malicious IoCs found in Indian Cyberspace related to APT SideCopy.

**IOCs: IOC\_Adv2024Apr006.txt attached**

1. **Adv/2024/Apr/007**

It has been reported that adversaries are targeting government personnel using spoofed/compromised email IDs, malicious domains and phishing web pages.   The Spear-phishing email contains a HTML (Hyper Text Markup Language) file. Upon clicking, it opens a new tab with the Outlook email page. In the background, the attacker misguided the victim by a forged letter theme with the blurred background, forcing the victim to fill in the Gov/NIC email Password in order to view the letter.

**IOCs: IOC\_Adv2024Apr007.txt attached**

1. **Adv/2024/Apr/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\_Adv2024Apr008.txt attached**

1. **Adv/2024/Apr/009**

**Vulnerability in SiYuan**

A Server Side Cross Site Scripting (XSS) vulnerability has been discovered in SiYuan that allows execution of arbitrary commands on the server. The affected version is SiYuan version 3.0.3.

CVE ID: CVE-2024-2692 (Critical)

**Vulnerability in Totolink**

An improper access control vulnerability has been discovered in Totolink. The affected version is Totolink N350RT 9.3.5u.6265.

CVE ID: CVE-2024-0570 (Critical)

**Vulnerability in Totolink**

An information disclosure vulnerability has been discovered in Totolink. The affected version is Totolink T8 4.1.5cu.833\_20220905.

CVE ID: CVE-2024-0569 (Critical)

1. **Adv/2024/Apr/010**

It has been observed that Kimusky group is distributing malware disguised as an installer. The malware is a dropper that creates Endoor backdoor. The dropper has fabricated its version information and is signed with a valid certificate. When the dropper is executed, it creates a compressed file. WinRAR is used to decompress the file to create and execute the backdoor. The dropper executes the backdoor with the argument “install”. The backdoor copies itself into the “%USERPROFILE%\svchost.exe” path and registers itself to the Task Scheduler under the name “Windows Backup”. The Task Scheduler executes the backdoor with the “backup” argument, after which the backdoor accesses the Command & Control (C2) server. Endoor backdoor is developed in Golang and is capable of sending basic information about the infected system, with features such as command execution, file upload and download, process-related tasks, and Socks5 proxy.

**IOCs: IOC\_Adv2024Apr010.txt attached**

1. **Adv/2024/Apr/011**

It has been reported that adversaries are targeting government personnel using spoofed/compromised email IDs, malicious domains and phishing web pages.   The Spear-phishing email contains a hyperlink. Upon clicking, it opens a phishing page and asks for username and password. The IP address on which the domain is hosted is malicious and currently active to potentially compromise the user credentials/propagate malware payload.

**IOCs: IOC\_Adv2024Apr011.txt attached**

1. **Adv/2024/Apr/012**

Presence of various ransomware variants are found in Indian Cyberspace.

The Ransomware variants include - Dyamond, Qilin, LockBit 3.0, Mallox & Cactus.

**IOCs:**

IOC\_Adv2024Apr012.txt

IOC\_Adv2024Apr012\_Dyamond.txt

IOC\_Adv2024Apr012\_Qilin.txt

IOC\_Adv2024Apr012\_Lockbit3.0.txt

IOC\_Adv2024Apr012\_Mallox.txt

IOC\_Adv2024Apr012\_Cactus.txt

1. **Adv/2024/Apr/013**

Presence of malicious IoCs found in Indian Cyberspace.

**IOCs: IOC\_Adv2024Apr013.txt attached**

1. **Adv/2024/Apr/014**

It has been observed that a backdoor in the upstream xz/liblzma software package has raised concerns about the security of \*nIX Systems i.e. Xenix, Linux, Ultrix, AIX, HP-UX, Irix Minix, and other non-ix ending systems like SunOS & BSD. The malicious code vulnerability (CVE-2024-3094) was found in the release tarball of the xz package, which is widely used in various Linux distributions for compressing data. The vulnerability causes SSH backdoor, inserted by a rogue developer, poses a significant threat as it allows unauthorized access to systems.

* **Mitigating the Risks associated with \*nix backdoor:-**

1. **Regular Security Audits:** Conduct routine audits of \*nIX System logs and monitor network traffic to detect any suspicious activity associated with the backdoor.
2. **Strong Authentication Mechanisms:** Implement robust authentication methods such as key-based authentication or multifactor authentication to ensure only authorized individuals can access the \*nIX System.
3. **Regular Updates and Patches:** Stay up-to-date with software updates and promptly apply patches to address any vulnerabilities or backdoor discovered in upstream xz/liblzma.
4. **Intrusion Detection Systems:** Deploy intrusion detection systems to actively monitor network traffic and detect any attempts to exploit the backdoor or compromise \*nIX System security.
5. **Network Segmentation:** Implement network segmentation to isolate the \*nIX System from other critical systems, limiting the potential lateral movement of attackers.
6. **Least Privilege Principle:** Employ the principle of least privilege by granting users only the necessary permissions required to perform their tasks on the \*nIX System. This reduces the potential impact of a backdoor compromise.
7. **Regular Backup and Recovery:** Create regular backups of \*nIX System data and develop a thorough incident response plan to enable swift recovery in the event of a compromise.

* **Common Signs and Indicators to identify the presence of a backdoor in a compromised system:**

1. **Unusual Network Traffic:** This indicates unauthorized communication or data exfiltration through the backdoor.
2. **Suspicious Log Entries:** Monitor system logs for any suspicious entries. Look for logins from unknown or unauthorized IP addresses, multiple failed login attempts, or any abnormal activities performed by system users.
3. **High CPU or Network Usage:** Excessive CPU or network usage can be a red flag. If noticed, a significant increase in resource utilization without any valid explanation, investigate further for possible backdoor exploitation.
4. **Unwanted Modifications:** Keep an eye out for unauthorized modifications to critical system files, directories, or configurations.
5. **Unexpected Processes or Services:** Identify any unknown or unusual processes or services running on your system.
6. **Suspicious Outgoing Connections:** Monitor outgoing connections from your \*nIX System. Look for unauthorized connections to unfamiliar IP addresses or suspicious domains that may indicate data exfiltration or unauthorized access attempts.
7. **Abnormal Behavior of User Accounts:** Be vigilant about the behavior of user accounts on your system. Look for any suspicious activities associated with privileged accounts, such as unauthorized modifications, unusual commands executed, or changes in access privileges.
8. **Security Software Alerts:**Security software, such as intrusion detection systems or antivirus programs, can provide alerts if they detect any suspicious activities related to the backdoor. Stay updated with the latest security software and promptly respond to any alerts generated.

* **Implementing Security Best Practices for \*nix System:-**

1. **Harden \*nIX System Configuration:** Configure your \*nIX System with strong security measures. Use strong passwords or, preferably, key-based authentication. Disable root login and enforce strict password policies to prevent unauthorized access.
2. **Implement Network and Firewall Security Measures:** Utilize firewalls to restrict access to \*nIX System. Consider implementing network segmentation and using intrusion detection systems to detect and prevent any unauthorized access attempts.
3. **Apply User Access Controls and Privilege Management:**Enforce the least privilege principles by granting users only the necessary permissions.
4. **Audit and Monitor:** Regularly monitor the system and log files for any unusual activities. Implement auditing mechanisms to detect any suspicious behavior related to the backdoor.
5. **Conduct Regular Security Assessments:** Perform regular security assessments to identify any vulnerabilities or weaknesses in \*nIX System configuration.
6. **Develop an Incident Response Plan:** Prepare an incident response plan in case of a backdoor compromise. This plan should include steps to isolate affected systems, restore from clean backups, and notify relevant authorities or stakeholders.
7. **Adv/2024/Apr/015**

It has been observed that there is an increase in malicious activity targeting Virtual Private Network (VPN) services. Adversaries use an array of malicious activity ranging from Secure Shell (SSH) brute forcing to Transport Layer Security (TLS) / Secure Sockets Layer (SSL) crawling associated with these anonymization services.

Adversaries are initially scanning and doing brute force activity, sourcing from The Onion Router (TOR) exit nodes and other anonymous tunnels and proxies. The successful attacks result in unauthorized access to a target network and lead to account lockouts and Denial of Service (DoS)-like conditions.

The targeted devices that fall into the following categories are:

    • Cisco Secure Firewall VPN

    • Checkpoint VPN

    • Fortinet VPN

    • SonicWall VPN

    • RD Web Services

(Although the list of impacted VPN services may be broader)

The brute force attempts to include a combination of generic usernames and valid usernames unique to specific organizations. The activity seems indiscriminate and has been observed across multiple industry verticals and geographic regions. Source IP addresses are generally tied to one of several proxy services, which include, but are not limited to:

    • TOR

    • VPN Gate

    • IPIDEA Proxy

    • BigMama Proxy

    • Space Proxies

    • Nexus Proxy

    • Proxy Rack

**IOCs: IOC\_Adv2024Apr015.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.
* Enable logging to a remote syslog server for improved correlation and auditing of network and security incidents across various network devices.
* Prevent authentication attempts and remote access VPN session establishment using default connection profiles/tunnel groups by pointing to a sinkhole AAA server.
* Implement an interface-level ACL on the ASA/FTD to filter out unauthorized public IP addresses and prevent them from initiating remote VPN sessions.
* Implement a control-plane ACL on the ASA/FTD to filter out unauthorized public IP addresses and prevent them from initiating remote VPN sessions.
* Organisation may use certificate-based authentication for Remote Access VPN (RAVPN), which provides a more robust approach compared to the use of credentials. To harden the environment, may change the authentication method for RAVPN to be based on certificates.

1. **Adv/2024/Apr/017**

**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-2024-20758 (Critical), CVE-2024-20759 (High), CVE-2024-20772 (High), CVE-2024-20771 (Medium), CVE-2024-20798 (Medium), CVE-2024-20797 (High), CVE-2024-20795 (High), CVE-2024-20796 (Medium), CVE-2024-20794 (Medium), CVE-2024-20737 (Medium), CVE-2024-20770 (Medium), CVE-2024-26047 (Medium), CVE-2024-26076 (Medium), CVE-2024-26079 (Medium), CVE-2024-26084 (Medium), CVE-2024-26087 (Medium), CVE-2024-26097 (Medium), CVE-2024-26098 (Medium), CVE-2024-26122 (Medium), CVE-2024-20778 (Medium), CVE-2024-20779 (Medium), CVE-2024-20780 (Medium), CVE-2024-26046 (Medium)

**Microsoft Released March 2024 Security Updates**

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

**Fortinet Released Security Updates for Multiple Products**

Fortinet has released security updates to address vulnerabilities in FortiClientMac, FortiClient Linux, FortiOS & FortiProxy. An attacker can exploit some of these vulnerabilities to take control of an affected system.

CVE ID: CVE-2023-45590 (Critical), CVE-2023-45588 (High), CVE-2024-31492 (High), CVE-2023-48784 (Medium), CVE-2023-41677 (High), CVE-2024-23662 (High)

1. **Adv/2024/Apr/018**

It has been observed that Curious Serpens aka Peach Sandstorm, APT33, Elfin, HOLMIUM, MAGNALIUM or REFINED KITTEN, an espionage group, has added FalseFont backdoor to compromise systems. The FalseFont backdoor is written in ASP.NET Core and has the following capabilities:

    • Executing processes and commands on the infected machine

    • Manipulating the file system

    • Capturing the screenshots

    • Stealing credentials from browsers browser's information

    • Stealing sensitive data for cyber espionage

FalseFont backdoor uses ASP.NET Core SignalR, which is an open-source library for running web applications and for communicating with its Command and Control (C2) server.

The GUI of the backdoor is active for user interaction while in the background multiple malware components are running. The FalseFont executable presents a login interface impersonating a legitimate company’s portal.  If a victim enters a username and password, the malware sends this data in JSON format through an HTTP POST request to the threat actor's C2 server over TCP port 8080. The threat actor for the initial infection mimicked the legitimate human resources software, using a fake job recruitment process to trick victims into installing the backdoor.

**IOCs: IOC\_Adv2024Apr018.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.
* Install update and patches regularly.
* Install and regularly update antivirus software.
* Implement a data backup and recovery plan.
* Implement Multi-Factor Authentication (MFA).
* Never run unknown files with exaggerated titles.
* Never open links shared on social media from unknown sources.
* Never click and execute email attachments from unknown sources.
* Users should take care when enabling macros for internal office files.

1. **Adv/2024/Apr/019**

Reference is made to earlier NCIIPC advisory Adv/2023/Oct/047 dated 31 Oct 2023 with subject- Operation Jacana.

It has been observed that Red Hat and Ubuntu systems are targeted by a Linux version of the DinodasRAT also known as Xdealer. Adversary creates a hidden file in the directory where its binary resides, which acts as a mutex to prevent multiple instances from running on the infected device. The malware set persistence on the computer using SystemV or SystemD startup scripts.

DinodasRAT shares system details with a Command and Control (C2) server to manage victim hosts. The communication with the C2 server occurs via TCP or UDP, utilizing Tiny Encryption Algorithm (TEA) in CBC mode. DinodasRAT has capabilities designed to monitor, control, and exfiltrate data from compromised systems.

**IOCs: IOC\_Adv2024Apr019.txt attached**

1. **Adv/2024/Apr/020**

Reference is made to earlier NCIIPC advisories on WarzoneRAT malware.

It has been observed that WarZoneRAT is again active with its tax-themed spam emails campaign. The compress attachment contains a LNK file that downloads an HTA file, initiating a Powershell command to download a malicious VBScript file. The VBScript then downloads and executes the next-stage Powershell payload, which further injects the final payload utilizing Reflective-loading technique to establish connection with a Command & Control (C2) server. Reflective loading technique is a technique that allows an attacker to inject a DLL's into a victim's process from memory rather than disk.

In another case, a compressed attachment contains an executable file, which, upon execution, loads the malicious WarzoneRAT DLL module using sideloading techniques. WarzoneRAT initiates malicious activities on the victim’s machine, establishing a connection to the C2 server.

**IOCs: IOC\_Adv2024Apr020.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.
* Install update and patches regularly.
* Install and regularly update antivirus software.
* Implement a data backup and recovery plan.
* Implement Multi-Factor Authentication (MFA).
* Allow only trusted applications to run on systems which prevent unauthorised applications from sideloading malicious DLLs.
* Use file integrity monitoring tools to detect changes to DLL files in critical directories. Any unexpected modifications can be a sign of a potential DLL sideloading attempt.
* Restrict access to directories where DLLs are loaded to prevent unauthorised modifications.
* Educate users about the risks of downloading and running files from untrusted sources, and the dangers of using outdated software.
* Implement robust endpoint security solutions that can detect and prevent suspicious activities, including DLL sideloading.

1. **Adv/2024/Apr/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\_Adv2024Apr021.txt attached**

1. **Adv/2024/Apr/022**

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\_Adv2024Apr022.txt attached**

1. **Adv/2024/Apr/023**

Presence of various phishing domains have been found in Indian Cyberspace.

**IOCs: IOC\_Adv2024Apr023.txt attached**

1. **Adv/2024/Apr/024**

Presence of various Advanced Persistent Threats (APTs) such as Imperial Kitten, POISONPLUG & Earth Krahang are found in Indian Cyberspace.

**IOCs: IOC\_Adv2024Apr024\_Imperial\_Kitten.txt attached**

**IOC\_Adv2024Apr024\_POISONPLUG.txt attached**

**IOC\_Adv2024Apr024\_Earth\_Krahang.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.
* Install and regularly update antivirus software.
* Install Updates and Patched regularly.
* Conduct regular backup practices and keep those backups offline or on a separate network.
* Implement Multi-Factor Authentication (MFA).

1. **Adv/2024/Apr/025**

**Multiple Vulnerabilities in Siemens Products:**

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

CVE ID: CVE-2023-35980 (Critical), CVE-2023-35981 (Critical), CVE-2023-35982 (Critical), CVE-2023-42789 (Critical), CVE-2024-21762 (Critical), CVE-2024-23113 (Critical), CVE-2023-45614 (Critical), CVE-2023-45615 (Critical), CVE-2023-45616 (Critical)

1. **Adv/2024/Apr/026**

It has been observed that threat actors are deploying Ramnit Trojan, a malware that is able to exfiltrate sensitive data such as banking credentials, FTP passwords, session cookies and personal data. Initially, the victim receives a spearphishing email that contains a link of a compromised website. Once the victim connects with a compromised website, the site initiates the download of an additional payload. This payload is a compressed ZIP file that contains a non-malicious .jpg file and a .lnk shortcut file. When the target opens the .lnk shortcut file, a CMD spawns a PowerShell with obfuscated commands. The PowerShell spawned by opening the .lnk file downloads the sLoad dropper.  sLoad is a PowerShell-based banking Trojan downloader with capabilities of reconnaissance, information gathering, screen capturing, and connecting to Command & Control (C2) for further communications. The downloader starts download by executing a PowerShell command that creates an empty .ps1 file. The malicious PowerShell script uses BITSAdmin to download sLoad and write it to the empty .ps1 file. BITSAdmin is a built-in Windows command-line tool for downloading, uploading, and monitoring jobs. Once the malicious PowerShell script is done writing sLoad into the .ps1 file, the file is executed. The malicious PowerShell script creates a scheduled task.  The payload of the BITSAdmin download is a Ramnit banking Trojan.

In execution, the Ramnit banking Trojan initiates its malicious activity through one of its persistence techniques used by trojan to minimize detection is living off the land binaries (LOLbins). It creates scheduled tasks through the COM API that uses the WMI process wmiprvse.exe.  Threat actors have used a combination of built-in Windows products including PowerShell, BITSAdmin, and certutil to avoid detection.

**IOCs: IOC\_Adv2024Apr026.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.
* Install update and patches regularly.
* Install and regularly update antivirus software.
* Implement a data backup and recovery plan.
* Implement Multi-Factor Authentication (MFA).
* Never run unknown files with exaggerated titles.
* Never open links shared on social media from unknown sources.
* Never click and execute email attachments from unknown sources.
* Users should take care when enabling macros for internal office files.

1. **Adv/2024/Apr/027**

It has been observed that attackers are exploting command injection vulnerability (CVE-2024-3400) which affects Palo Alto Network's firewalls. The vulnerability has been given a CVSSv4.0 score of 10.

CVE-2024-3400 is a command injection vulnerability in the GlobalProtect feature of Palo Alto Networks PAN-OS software which allows unauthenticated attacker to execute arbitrary code with root priveleges on vulnerable firewalls.

GlobalProtect gateway configuration can be checked in firewall web interface (Network-> GlobalProtect->Gateways) and configuration of telemetry can be checked (Device-> Setup-> Telemetry)

**Vulnerable Products:**

The vulnerability affects PAN-OS versions 11.1, 11.0 and 10.2 that have configurations for both GlobalProtect gateway and device telemetry enabled.

**Solution:**

This issue will be fixed in hotfix releases of PAN-OS 10.2.9-h1, PAN-OS 11.0.4-h1, and PAN-OS 11.1.2-h3 which are scheduled to be released on 14 April 2024.

**IOCs: IOC\_Adv2024Apr027.txt attached**

**Recommendations/Mitigations:**

* 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.
* Organisation must ensure vulnerability protection has been applied to their GlobalProtect interface to prevent exploitation of this issue on their device.
* Impact of this vulnerability can be mitigated by temporarily disabling device telemetry until the device is upgraded to a fixed PAN-OS version. Once upgraded, device telemetry should be re-enabled on the device.
* Install updates and patches as soon as it available.

1. **Adv/2024/Apr/029**

**Vulnerability in Ai3 QbiBot**

A vulnerability has been discovered in the password reset feature of Ai3 QbiBot due to lack of proper access control that allows adversaries to reset any user's password.

CVE ID: CVE-2024-3777 (Critical)

**Palo Alto Networks Released Security Updates**

Palo Alto Networks has released security updates to resolve a command injection vulnerability in the GlobalProtect feature of Palo Alto Networks PAN-OS. The affected versions are PAN-OS 10.2, PAN-OS 11.0, and PAN-OS 11.1.

CVE ID: CVE-2024-3400 (Critical)

**Juniper Networks Security Updates**

Juniper Networks has released security updates to address multiple vulnerabilities in Juniper Networks Junos OS and Junos OS Evolved.

CVE ID: CVE-2023-38545 (Critical), CVE-2023-38546 (Low), CVE-2023-23914 (Critical), CVE-2023-23915 (Medium), CVE-2020-8284 (Low), CVE-2020-8285 (High), CVE-2020-8286 (High), CVE-2018-1000120 (Critical), CVE-2018-1000122 (Critical)

1. **Adv/2024/Apr/030**

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\_Adv2024Apr030.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/Apr/031**

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\_Adv2024Apr031.txt attached**