**Cyber Security Advisories**

**Date: 31 July 2024**

1. **Adv/2024/Jul/038**

It has been observed that a Signal Handler Race Condition vulnerability tracked as CVE-2024-6409 exists in OpenSSH impacting Red Hat Enterprise Linux 9. Exploitation of this vulnerability could allow attackers to gain unauthorized access to systems, execute malicious commands, exfiltrate sensitive data, or launch further attacks within the network. The race condition and RCE potential are triggered in the privsep child process, which runs with reduced privileges compared to the parent server process.

The race condition vulnerability CVE-2024-6387 affects OpenSSH server component. When succesfully exploited, it allows an attacker to execute arbitrary code with the highest privileges on Linux systems that rely on the GNU C Library (glibc), subvert security mechanisms, data theft, and even maintain persistent access.

**Reference:** CERT-IN [CMTX-P072024075]

https://access.redhat.com/security/cve/CVE-2024-6409

1. **Adv/2024/Jul/039**

Reference is made to earlier advisories on the above subject.

It has been observed that APT40 (also known as Kryptonite Panda, GINGHAM TYPHOON, Leviathan and Bronze Mohawk) has the ability to use proof-of-concepts (POCs) of new vulnerabilities to attack networks that have a vulnerable infrastructure. It regularly scans networks, to find and exploit vulnerable, outdated, end-of-life or no longer maintained devices on networks to rapidly deploy exploits. It exploits vulnerabilities in widely used software such as Log4J (CVE 2021 44228), Atlassian Confluence (CVE-2021-31207, CVE-2021-26084) and Microsoft Exchange (CVE-2021-31207; CVE-2021-34523; CVE-2021-34473).  It uses web shells for persistence. It compromises devices, including Small Office/Home Office (SOHO) devices.

APT40 is capable of performing:-

• Host enumeration, which enables threat actors to build their own map of the network;

• Web shell use, giving adversaries an initial foothold on the network and a capability to execute commands; and

• Deployment of other tools leveraged by the threat actor for malicious purposes.

**IOCs: IOC\_Adv2024Jul039.txt attached**

1. **Adv/2024/Jul/040**

It has been observed that critical remote code execution vulnerability tracked as CVE-2024-4577 is a PHP vulnerability that affects installations running CGI mode. Threat actors such as Gh0st RAT, RedTail cryptominers, XMRig are exploiting this vulnerability. The vulnerability is caused due to the way, PHP and CGI handlers parse certain Unicode characters, which enable attackers to achieve remote code execution (RCE).

**AFFECTED VERSION:**

PHP (versions 8.1.\*, before 8.1.29, 8.2.\* before 8.2.20, and 8.3.\* before 8.3.8)

**IOCs: IOC\_Adv2024Jul040.txt attached**

1. **Adv/2024/Jul/042**

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\_Adv2024Jul042.txt attached**

1. **Adv/2024/Jul/043**

Various Microsoft 365 application and services are reported to have been impacted with “Blue Screen of Death” (BSOD) error that caused user systems to shut down or restart and resulted in disruption in operations in Critical Sector Entities (CSEs).

As per Microsoft issued advisory, the preliminary root cause for this is the “Configuration change” in a portion of its Azure backend workloads which caused interruption between storage and compute resources that resulted in connectivity failures affecting Microsoft 365 services. As per Microsoft, the issue of impacting Virtual Machines (VM) running Windows Client and Windows Server is due to the running of the CrowdStrike Falcon agent, which may have encountered a bug check (BSOD) and get stuck in a restarting state.

**CSEs are advised to do the following for all the Critical Systems / Networks:**

1. Boot Windows into Safe Mode or the Windows Recovery Environment to restore to the known good state or last restore point.

2. Once the disk is attached, customers can attempt to delete the following file. Windows/System/System32/Drivers/CrowdStrike/C00000291\*.sys.The disk can then be attached and re-attached to the original VM.

3. Only OEM recommended fixes to be applied after testing on the staging platform.

4. Restore point for the last good state may be created for all the critical services.

5. Update the Critical systems in phased manner based on the risk profile.

6. CSE’s are advised to deploy sufficient skilled manpower to monitor, any degradation of services due to any dependency.

7.    In case you are using the EDR solutions from these OEMs, kindly keep the SoC on high alert to monitor any attempt of cyber-attack during restoration phase.

**References:**

* https://status.cloud.microsoft/
* https://learn.microsoft.com/en-us/azure/backup/backup-azure-arm-restore-vms
* https://learn.microsoft.com/en-us/troubleshoot/azure/virtual-machines/windows/unlock-encrypted-disk-offline
* https://learn.microsoft.com/en-us/troubleshoot/azure/virtual-machines/windows/unmanaged-disk-offline-repair

1. **Adv/2024/Jul/044**

Reference is made to earlier advisory on the above subject.

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

**IOCs: IOC\_Adv2024Jul044.txt attached**

1. **Adv/2024/Jul/045**

It has been observed that JRat malware is active in the cyber threat landscape.

The campaign begins with a spear-phishing email containing a ZIP attachment. The attachment contains JS, VBS, or JAR-based malware. Once the user opens the attachment, the malicious payload executes and persists itself. Upon execution, the file transforms into a remote admin tool (JRat), which takes over the victim’s device, communicates with the C2 server, executes remote commands, and spreads across the network.

**IOCs: IOC\_Adv2024Jul045.txt attached**

**Measures for prevention & detection of these attacks:**

**1. Detection measures**

a) Enable Event logging and Monitoring focusing on Adversarial Activities such as:

        1.Monitor for brute-force attempts. Check excessive failed authentication attempts.

        2.Monitor for clearing of Event Logs, especially the Security Event log and PowerShell Operational logs.

b) Use process monitoring to monitor the execution and arguments of mshta.exe. Mshta can execute Windows Script Host code (VBScript and JScript).

c) Monitor antivirus alerts and event logs for detection of any malicious.

**2. Protection Measures**

a)  Establish a Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and Domain Keys.

b) Disable or remove java, if not required, within a given environment.

c) All operating systems and applications should be updated on a regular basis. Virtual patching can be considered for protecting legacy systems and networks.

d) Deploy web and email filters on the network. Configure these devices to scan for known bad domains, sources, and addresses; block these before receiving and downloading messages. Scan all emails, attachments, and downloads both on the host and at the mail gateway with a reputable antivirus solution.

e) Enforce application whitelisting on all endpoint workstations which allows execution of only known/genuine programs.

f) Network segmentation and segregation into security zones help protect sensitive information and critical services.

g) Turn on attack surface reduction rules, including rules that block credential theft, ransomware activity, and suspicious use of PsExec and WMI.

h) Utilize the Windows Defender Firewall and your network firewall to prevent RPC and SMB communication among endpoints whenever possible. This limits lateral movement as well as other attack activities.

1. **Adv/2024/Jul/046**

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\_Adv2024Jul046.txt attached**

1. **Adv/2024/Jul/047**

Reference is made to earlier advisories on Racoon Malware.

Raccoon, an info stealer malware, is available as a Malware as a Service (MaaS). The malware has the capability to check system settings, capture screenshots, collect basic information like OS version, IP & username and steal passwords & logins from a variety of browsers.

PFA additional IOCs in this regard.

**IOCs: IOC\_Adv2024Jul047.txt attached**

1. **Adv/2024/Jul/048**

Presence of malicious IoCs are found in Indian Cyberspace related to various malwares i.e. KEYPLUG, ShadowPad and SOGU/PlugX.

PFA IOCs in this regard.

**IOCs: IOC\_Adv2024Jul048.txt attached**

1. **Adv/2024/Jul/049**

Reference is made to earlier advisories on Trickbot Malware.

Trickbot is a highly modular malware, capable of performing a number of actions on a network, such as stealing information or dropping ransomware.

**IOCs: IOC\_Adv2024Jul049.txt attached**

1. **Adv/2024/Jul/050**

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\_Adv2024Jul050.txt attached**