**21 Apr 25**

# Cyber Threat Roundup

***A collection of recent open-source items of interest to the Defense Industrial Base***

## Contents

# Articles

## Gladinet's Triofox and CentreStack Under Active Exploitation via Critical RCE Vulnerability

A recently disclosed security flaw in Gladinet CentreStack also impacts its Triofox remote access and collaboration solution, according to Huntress, with seven different organizations compromised to date. Tracked as CVE-2025-30406 (CVSS score: 9.0), the vulnerability refers to the use of a hard-coded cryptographic key that could expose internet-accessible servers to remote code execution attacks. It has been addressed in CentreStack version 16.4.10315.56368 released on April 3, 2025. The vulnerability is said to have been exploited as a zero-day in March 2025, although the exact nature of the attacks is unknown.

https://thehackernews.com/2025/04/gladinets-triofox-and-centrestack-under.html

## Critical Flaws Fixed in Nagios Log Server

The Nagios Security Team has fixed three critical vulnerabilities affecting popular enterprise log management and analysis platform Nagios Log Server. The vulnerabilities, discovered and reported by security researchers Seth Kraft and Alex Tisdale, include: a stored XSS vulnerability (CVE-2025-29471) in the web interface of Nagios Log Server that allows a standard (low-privilege) user to inject a malicious JavaScript payload into their profile's 'email' field to achieve privilege escalation; A DoS vulnerability (CVE pending) that could allow a non-admin users to shut down Elasticsearch; and an information disclosure vulnerability (CVE pending) that allows any low-level user (with API read-only access) to perform a "get_users" API request and grab API keys (tokens) for all read-only and admin users in plaintext. The vulnerabilities affect Nagios Log Server version 2024R1.3.1 and have been fixed in version 2024R2 and version 2024R1.3.2.

https://www.helpnetsecurity.com/2025/04/15/critical-flaws-fixed-in-nagios-log-server/

## Chinese Hackers Target Linux Systems Using SNOWLIGHT Malware and VShell Tool

The China-linked threat actor known as UNC5174 has been attributed to a new campaign that leverages a variant of a known malware dubbed SNOWLIGHT and a new open-source tool called VShell to infect Linux systems. UNC5174, also referred to as Uteus (or Uetus), was previously documented by Google-owned Mandiant as exploiting security flaws in Connectwise ScreenConnect and F5 BIG-IP software to deliver a C-based ELF downloader named SNOWLIGHT, which is designed to fetch a Golang tunneler dubbed GOHEAVY from infrastructure tied to a publicly available command-and-control (C2) framework known as SUPERSHELL. In the attack chain observed by Sysdig in late January 2025, the SNOWLIGHT malware acts as a dropper for a fileless, in-memory payload called VShell, a remote access trojan (RAT) widely used by Chinese-speaking cybercriminals.

https://thehackernews.com/2025/04/chinese-hackers-target-linux-systems.html

## Midnight Blizzard Deploys New GrapeLoader Malware in Embassy Phishing

Russian state-sponsored espionage group Midnight Blizzard is behind a new spear-phishing campaign targeting diplomatic entities in Europe, including embassies. According to Check Point Research, the new campaign introduces a previously unseen malware loader called 'GrapeLoader,' and a new variant of the 'WineLoader'

backdoor. The email contains a malicious link that, if the victim targeting conditions are met, triggers the download of a ZIP archive (wine.zip). The archive contains a legitimate PowerPoint executable (wine.exe), a legitimate DLL file required for the program to run, and the malicious GrapeLoader payload (ppcore.dll). The malware loader is executed via DLL sideloading, which collects host info, establishes persistence via Windows Registry modification, and contacts the command-and-control (C2) to receive the shellcode it loads in memory.

https://www.bleepingcomputer.com/news/security/midnight-blizzard-deploys-new-grapeloader-malware-in-embassy-phishing/

## Chinese Android Phones Shipped with Fake WhatsApp, Telegram Apps Targeting Crypto Users

Cheap Android smartphones manufactured by Chinese companies have been observed pre-installed with trojanized apps masquerading as WhatsApp and Telegram that contain cryptocurrency clipper functionality as part of a campaign since June 2024. While using malware-laced apps to steal financial information is not a new phenomenon, the new findings from Russian antivirus vendor Doctor Web point to significant escalation where threat actors are directly targeting the supply chain of various Chinese manufacturers to preload brand new devices with malicious apps.

https://thehackernews.com/2025/04/chinese-android-phones-shipped-with.html

## Oracle Patches 180 Vulnerabilities with April 2025 CPU

On April 15, Oracle announced the release of 378 new security patches as part of its second Critical Patch Update (CPU) of 2025, including 255 fixes for vulnerabilities that are remotely exploitable without authentication. For multiple products, Oracle did not release new security patches, but announced fixes for non-exploitable third-party CVEs. For other products, the fixes address additional CVEs and non-exploitable CVEs. Oracle customers are advised to apply the patches as soon as possible, as threat actors have been observed exploiting Oracle vulnerabilities for which fixes have been released but not applied.

https://www.securityweek.com/oracle-patches-180-vulnerabilities-with-april-2025-cpu/

## New BPFDoor Controller Enables Stealthy Lateral Movement in Linux Server Attacks

Cybersecurity researchers have unearthed a new controller component associated with a known backdoor called BPFDoor as part of cyber attacks targeting telecommunications, finance, and retail sectors in South Korea, Hong Kong, Myanmar, Malaysia, and Egypt in 2024. "The controller could open a reverse shell," Trend Micro researcher Fernando Mercês said in a technical report published earlier in the week. "This could allow lateral movement, enabling attackers to enter deeper into compromised networks, allowing them to control more systems or gain access to sensitive data.The campaign has been attributed with medium confidence to a threat group it tracks as Earth Bluecrow, which is also known as DecisiveArchitect, Red Dev 18, and Red Menshen.

https://thehackernews.com/2025/04/new-bpfdoor-controller-enables-stealthy.html

## New Windows Task Scheduler Bugs Let Attackers Bypass UAC and Tamper with Logs

Cybersecurity researchers have detailed four different vulnerabilities in a core component of the Windows task scheduling service that could be exploited by local attackers to achieve privilege escalation and erase logs to cover up evidence of malicious activities. The issues have been uncovered in a binary named "schtasks.exe," which enables an administrator to create, delete, query, change, run, and end scheduled tasks on a local or remote computer. “A [User Account Control] bypass vulnerability has been found in Microsoft Windows, enabling attackers to bypass the User Account Control prompt, allowing them to execute high-privilege (SYSTEM) commands without user approval," Cymulate security researcher Ruben Enkaoua said in a report shared with The Hacker News.

https://thehackernews.com/2025/04/experts-uncover-four-new-privilege.html

## Apple Fixes Two Zero-Days Exploited in Targeted iPhone Attacks

Apple released emergency security updates to patch two zero-day vulnerabilities that were used in an "extremely sophisticated attack" against specific targets' iPhones. The two vulnerabilities are in CoreAudio (CVE-2025-31200) and RPAC (CVE-2025-31201), with both bugs impacting iOS, macOS, tvOS, iPadOS, and visionOS. "Apple is aware of a report that this issue may have been exploited in an extremely sophisticated attack against specific targeted individuals on iOS," reads an Apple security bulletin.

https://www.bleepingcomputer.com/news/security/apple-fixes-two-zero-days-exploited-in-targeted-iphone-attacks/