2025-04-09 - News Report

# New TCESB Malware Found in Active Attacks Exploiting ESET Security Scanner

Summary:  
 A Chinese-affiliated threat actor known for its cyber-attacks in Asia has been observed exploiting a security flaw in security software. Kaspersky said its investigation into ToddyCat-related incidents in early 2024 unearthed a suspicious DLL file in the temp directory on multiple devices. The 64-bit DLL, TCESB, has been found to be launched via a technique called DLL Search Order Hijacking to seize control of the execution flow. This is said to have been accomplished by taking advantage of a flaw in the ESET Command Line Scanner. TCESB checks every two seconds for the presence of a payload file with a specific name in the current directory. payload artifacts are encrypted using AES-128 and are decoded and executed as soon as they appear in the specified path. exploited as part of BYOVD attacks by the North Korea-linked Lazarus Group to turn off security mechanisms. "To detect the activity of such tools, it's recommended to monitor systems for installation events involving drivers with known vulnerabilities," Kaspersky said.

Extracted Important Information:

* CVE: CVE-2024-11859
* CVE: CVE-2021-36276
* CVE: CVE-2021-21551
* CVSS: CVSS score: 6.8

Link: https://thehackernews.com/2025/04/new-tcesb-malware-found-in-active.html

# PipeMagic Trojan Exploits Windows Zero-Day Vulnerability to Deploy Ransomware

Summary:  
 Microsoft says a vulnerability in the Windows Common Log File System was exploited as a zero-day in ransomware attacks aimed at a small number of targets. The vulnerability in question is CVE-2025-29824, a privilege escalation bug in CLFS that could be exploited to achieve SYSTEM privileges. Microsoft is tracking the activity and the post-compromise exploitation of the vulnerability under the moniker Storm-2460. The threat actors also leveraging a malware named PipeMagic to deliver the exploit as well as ransomware payloads. "We're trying to make sure that we're not using ransomware within an environment," he says. "We're not trying to use it as a tool to get at the root of a problem," he adds. "It's just a way of trying to prevent it from happening in the first place. We don't want it to be a tool that's going to be used against us in the future," says the CEO of the company. "What we want to do is make sure we don't use it for the sake of it," adds the CEO.

Extracted Important Information:

* CVE: CVE-2025-29824
* CVE: CVE-2025-24983
* CVE: CVE-2023-28252

Link: https://thehackernews.com/2025/04/pipemagic-trojan-exploits-windows-clfs.html

# CISA Warns of CentreStack's Hard-Coded MachineKey Vulnerability Enabling RCE Attacks

Summary:  
 U.S. Cybersecurity and Infrastructure Security Agency (CISA) adds Gladinet CentreStack to its Known Exploited Vulnerabilities (KEV) catalog. The vulnerability, tracked as CVE-2025-30406, concerns a case of a hard-coded cryptographic key that could be abused to achieve remote code execution. There are currently no details on how the vulnerability is being exploited, the identity of the threat actors exploiting it, and who may be the targets of these attacks. That said, a description of the security defect on CVE.org says it was exploited in the wild in March 2025.

Extracted Important Information:

* CVE: CVE-2025-30406
* CVSS: CVSS score: 9.0

Link: https://thehackernews.com/2025/04/cisa-warns-of-centrestacks-hard-coded.html

# Microsoft Patches 126 Flaws Including Actively Exploited Windows CLFS Vulnerability

Summary:  
 Microsoft has released security fixes to address a massive set of 126 flaws affecting its software products. Of the 126 vulnerabilities, 11 are rated Critical, 112 are rated Important, and two are rated Low in severity. Forty-nine of these vulnerabilities are classified as privilege escalation, 34 as remote code execution, 16 as information disclosure, and 14 as denial-of-service (DoS) bugs. The updates are aside from the 22 flaws the company patched in its Chromium-based Edge browser since the release of last month's Patch Tuesday update. Several of the vulnerabilities are yet to receive patches for Windows 10. Microsoft said the updates would be "released as soon as possible" Patches have also been released by other vendors over the past few weeks to rectify several vulnerabilities. Other vendors include: Adobe, Amazon Web Services, AMD, Apache Parquet, Apple Arm, Bitdefender, Broadcom, HP Enterprise, Salesforce, SAP, Siemens, Sophos, and Zoho ManageEngine, and Zoom. The vulnerabilities are listed in the list of Critical flaws below.

Extracted Important Information:

* CVE: CVE-2025-29824
* CVE: CVE-2022-24521
* CVE: CVE-2022-37969
* CVE: CVE-2023-23376
* CVE: CVE-2023-28252
* CVE: CVE-2024-49138
* CVE: CVE-2025-29809
* CVE: CVE-2025-27480
* CVE: CVE-2025-27482
* CVE: CVE-2025-26663
* CVE: CVE-2025-26670
* CVE: CVE-2025-29791
* CVE: CVE-2025-27749
* CVE: CVE-2025-27748
* CVE: CVE-2025-27745
* CVE: CVE-2025-27752
* CVE: CVE-2025-26686
* CVE: CVE-2025-27491
* CVSS: CVSS score: 7.8

Link: https://thehackernews.com/2025/04/microsoft-patches-126-flaws-including.html