2025-04-08 - News Report

# Fortinet Urges FortiSwitch Upgrades to Patch Critical Admin Password Change Flaw

Fortinet has released security updates to address a critical security flaw impacting FortiSwitch. The vulnerability, tracked as CVE-2024-48887, carries a CVSS score of 9.3 out of a maximum of 10.0. As workarounds, Fortinet recommends disabling HTTP/HTTPS access from administrative interfaces and restricting access to the system to only trusted hosts. While there is no evidence that the vulnerability has been exploited, a number of security flaws affecting Fortinet products have been weaponized by threat actors.

Link: https://thehackernews.com/2025/04/fortinet-urges-fortiswitch-upgrades-to.html

# Cryptocurrency Miner and Clipper Malware Spread via SourceForge Cracked Software Listings

Kaspersky: Threat actors have been distributing malicious payloads via SourceForge. One such project, officepackage, contains Microsoft Office add-ins copied from GitHub. 90% of potential victims are in Russia, with 4,604 users encountering the scheme between early January and late March. The disclosure comes as the company revealed details of a campaign that's distributing a malware downloader called TookPS via fraudulent sites impersonating the SourceForge site. the website displays a long list of Microsoft Office applications and corresponding links to download them in Russian. The fact that the website has a Russian interface indicates a focus on Russian-speaking users. Malvertising remains a persistent and evolving threat. Google ads for RVTools deliver a tampered version that's laced with ThunderShell. TookPS is engineered to download and execute PowerShell scripts that grant remote access to the infected host via SSH, and drop a modified version of a trojan dubbed TeviRat. This highlights the threat actor's attempts to gain complete access to a victim's computer in a variety of ways.. DeepSeek artificial intelligence (AI) chatbot, as well as remote desktop and 3D modeling software.

Link: https://thehackernews.com/2025/04/cryptocurrency-miner-and-clipper.html

# UAC-0226 Deploys GIFTEDCROOK Stealer via Malicious Excel Files Targeting Ukraine

A new set of cyber attacks targeting Ukrainian institutions with information-stealing malware. The activity is aimed at military formations, law enforcement agencies, and local self-government bodies. The attacks involve distributing phishing emails containing a macro-enabled Microsoft Excel spreadsheet. The email messages are sent from compromised accounts, often via the web interface of email clients, to lend the messages a veneer of legitimacy, and trick prospective victims into opening the documents. It comes as a suspected Russia-nexus espionage actor dubbed UNC5837 has been linked to a phishing campaign targeting European government and military organizations in October 2024. The attack paves the way for the delivery and execution of an MSI installer file that's responsible for launching Legion Loader. Victims are redirected to a second Cloudflare Turnstile CAPTCHA that, upon completion, is redirected again to a page that provides ClickFix-style instructions to download the document they are looking for. The end goal is to capture a wide range of sensitive information and exfiltrate it to the attackers. The attack also terminates the browser session for the extension to be enabled, turns on developer mode in the settings, and relaunches the browser.

Link: https://thehackernews.com/2025/04/uac-0226-deploys-giftedcrook-stealer.html

# CISA Adds CrushFTP Vulnerability to KEV Catalog Following Confirmed Active Exploitation

CrushFTP has been added to the U.S. Cybersecurity and Infrastructure Security Agency's Known Exploited Vulnerabilities (KEV) catalog. The vulnerability is a case of authentication bypass that could permit an unauthenticated attacker to take over susceptible instances. It has been fixed in versions 10.8.4 and 11.3.1. The development comes after the disclosure process associated with the flaw has been entangled in controversy and confusion, with VulnCheck accusing CrushFTP of attempting to cover up the vulnerability. Huntress said it observed in-the-wild exploitation of CVE-2025-31161 on April 3, 2025. The cybersecurity firm said it has seen exploitation efforts targeting four distinct hosts from four different companies to date. The names of the impacted companies were not disclosed, but they belong to marketing, retail, and semiconductor sectors. As of April 6, 2025, there are 815 unpatched instances vulnerable to the flaw, with 487 of them located in North America and 250 in Europe.

Link: https://thehackernews.com/2025/04/cisa-adds-crushftp-vulnerability-to-kev.html