

Forum:[Hack Forums](#)

Thread: [Hack Forum News - Edition 24](#)

Mix - November 24, 2025, 10:44 am

Hack Forum News - Edition 24

Welcome back to the Hack Forum News. Where we keep you up to date on the weekly events and news happening on site and around the world. If you have never heard of the Hack Forum News, don't worry, we have you covered. We are a team of members from the Hack Forums community who are journalists and writers, and we are here to keep you in the loop of the changes around the site and the events happening around the world.

Writer - [Mix](#)

[The Hack Forums Wiki Returns](#) By [Mix](#)

The Hack Forums Wiki is back in action and is now under way to a few big changes. The site has been under some work recently as the site was sadly left with a load of issues and no one was running the official site. Thanks to everyone within the HF news team, the site is now under new leadership and, thanks to [Omniscient](#) allowing the team to start their work on this while maintaining the HF news, the site is back getting some lovely changes and getting updated daily to bring it back to a new modern day Wikipedia with a load of information for everyone to read up on.

[Vacation](#) By [Omniscient](#)

[Omniscient](#) has recently just come back from their vacation in Santa Barbara, California. They have shared with us their experience going there and have said that it wasn't too far from home and they would go again. He has also mentioned that this is his first vacation they have had in a little while and shared some lovely pictures of the place while he was away.

[Hack Forums News Team - Become a Writer](#) By [Mix](#)

Are you looking to join the HF news team? Do you enjoy making threads or even want to become a better writer? Well, we are looking for members of the site to help write each week and are looking for anyone who has any interest. We have a few new sections opening up right now, and we would love for you to see if they would be anything of interest to you. If you are interested, please check out the thread or contact Mix to discuss joining the team behind the HF News.

Writer - [Mix](#)

Last Week:

Spoiler ([Click to View](#))

Writer - [Mix](#)

[Confound](#) Has obtained the "King Decade" award -

[Flaws](#) Has obtained the "King Decade" award -

[G33K](#) Has obtained the "King Decade" award -

[zavierd](#) Has obtained the "King Decade" award -

[Wilmer](#) Has obtained the "Flip Reaper" award -

Writer - [Oh_Well](#)

[Sign Language and Carpal Tunnel](#) - by [Tyr](#)

[Tyr](#) opens a thoughtful discussion about the physical toll of learning and practicing ASL. Members who sign, or who simply spend long hours on a keyboard, jump in to share wrist pain experiences, remedies, and ways to keep progressing even when the hands protest. A wholesome and practical thread for anyone dealing with carpal tunnel or hand strain.

[\[Quantum\] The Ultimate Prompt Engineering Guide \(2025 Edition\)](#) - by [????????????](#)

A massive, high-effort drop, packed with techniques, blueprints, multi-step workflows, simulation strategies, anti-hallucination rules, and advanced examples for mastering AI systems. Whether you write, code, research, or automate, this guide is basically a full textbook on modern prompt engineering. Easily one of the most comprehensive resources posted on HF this year.

[Google's Antigravity](#) - by [Hackers](#)

[Hackers](#) highlights Google's new agentic development platform, Antigravity, and what it means for the future of work. The message is blunt: if you're still judging AI by a simple chat box, you're already outdated. With deep app integration and automated workflows, this tech is reshaping how fast individuals can build and ship. A wake-up call thread for anyone sleeping on modern AI tools.

[1,000,000 Bytes Sports Bet](#) - by [Mooooookie](#)

[Mooooookie](#) shares a wild gambling comeback—dropping a million Bytes on sports betting and actually winning after losing the same amount earlier this year. Screenshots included. A fun, high-stakes moment that has the community cheering, cringing, and celebrating the dub.

[Wishing you all a wonderful day](#) - by [HerrWinston](#)

A wholesome reminder that progress doesn't require perfection. Whether you're having a great day or a rough one, this thread is pure positivity and good vibes, complete with hopes for a snowy Christmas. A small but welcome moment of warmth on HF.

[Whats something you're genuinely excited about in your life right now?](#) - by [Flariuu](#)

[Flariuu](#) asks one of those simple questions that turns into a feel-good community moment: what's something you're excited about these days? From small wins to new hobbies-like scuba diving-the thread is full of members sharing what's keeping them motivated and moving forward.

Writer - [Chrome](#)

GROUPS FOR SALE AND SOLD

[Succubus group](#) is still listed for sale by [SecretAchiever101](#)
[Olympians group & Benevolence](#) are still listed for sale by [Neil](#)

[Mystery Inc](#) listed for sale by [Scooby](#)

RECENT GROUP CHANGES & EVENTS

[xadamxk](#) has been added as leader to Sociopaths

RECRUITMENTS:

[Casino Recruitment](#)
[Pink LSZ Recruitment](#)
[Warriors Recruitment](#)
[Gamblers Recruitment](#)
[Legends Recruitment](#)
[Allegiance Buy-in](#)
[Olympians leader recruitment](#)
[The Academy Recruitment](#)

Writer - [Mix](#)

Recently we introduced a brand-new section to the HF News. This section will grow over time to more things, but for now we are just going to be doing Song of the week. We are open to what more we could bring to the section from your suggestions, but as a start, we feel adding the song of the week will be a great start for the section and lead the way forward for more things in the future.

Now we know some of you may question what the song of the week is all about, and we have thought of what a great answer. We feel like the song of the week should be a meaningful song that goes deeper than just general music and has meaning to it all. Granted, we may have a little fun with it sometimes. (Yes, we will have a Halloween version and Christmas version too.) But we want to keep it at a level where we have found the song has a true message behind it all and not just something that everyone will just see as another song that is just a bit catchy or got a good few beats to it. We hope this helps those with that question and if anyone has anything that they wish to ask, please feel free to add them below. We are more than happy to give the reason behind it.

This weeks Song Of The Week:

[Video: <https://youtu.be/oNjQXmoxiQ8>]

Big thank you to [Hackers](#) For this weeks submission.

Writer - [Mix](#)

[\\$50 USD BTC GIVEAWAY || ANYONE CAN ENTER!! || ONE ENTRY ONLY](#) By [Flariuu](#)

A member known as [Flariuu](#) is hosting a giveaway that will end on the 1st of December 2025 and is giving away \$50 worth of BTC. Anyone can enter and you all will have the same chance to win. Go see if you can get lucky.

[\\$25 CRYPTO GIVEAWAY — YOUR CHOICE](#) By [Vectura](#)

[Vectura](#) has started a giveaway that will end on the 25th of November this year and is giving away \$25 of crypto of your liking to the winner. Go and see if you can get lucky and win some free crypto.

Writer – [????????????](#)

Fortinet confirms second FortiWeb zero-day (CVE-2025-58034) exploited in the wild
Fortinet has acknowledged a second zero-day in its FortiWeb WAF being actively exploited. The vulnerability allows authenticated attackers to execute OS commands via crafted HTTP or CLI inputs.

[Source](#)

Critical FortiWeb path-traversal bug now actively exploited, warns CybersecAsia
CybersecAsia reports that CVE-2025-64446 in FortiWeb is being abused by unauthenticated attackers to create admin accounts due to a path-traversal/authentication bypass.

[Source](#)

FortiWeb authenticated OS command injection bug (CVE-2025-58034) confirmed; patch now available

Censys advisory confirms CVE-2025-58034 impacts FortiWeb and has been actively exploited; Fortinet urges users to patch to version 8.0.2 or higher.

[Source](#)

NHS England reports widespread FortiWeb path-traversal exploit being actively attacked
NHS England's cybersecurity team warns that multiple FortiWeb devices are under active exploit via CVE-2025-64446, urging immediate patching or mitigations.

[Source](#)

CISA adds FortiWeb zero-day (CVE-2025-64446) to its KEV list following exploitation reports
National Cyber Security Authority alerts show that CVE-2025-64446 was added to regarded as a known exploited vulnerability, with multiple attacks already recorded.

[Source](#)

CYFIRMA weekly intelligence: DigitStealer macOS malware trending, Volt Typhoon espionage signals rise

In its November 21 intelligence report, CYFIRMA highlights "DigitStealer" for macOS credential theft and reports escalating Volt Typhoon activity targeting allied infrastructure.

[Source](#)

Cloudflare outage disrupts major internet services, study shows key infrastructure risk
A global Cloudflare outage caused service disruptions and error messages across the internet. Experts warn about the growing risk of centralized infrastructure failures.

[Source](#)

Writer - [MadScientist](#)

Critical Oracle Identity Manager Flaw Potentially Exploited as Zero-Day

Searchlight Cyber on Thursday disclosed a severe vulnerability in Oracle Identity Manager, tracked as CVE-2025-61757, after identifying and reporting the issue to Oracle.

The flaw is characterized as a critical pre-authentication remote code execution (RCE) vulnerability, enabled through a chained exploit involving an authentication bypass followed by arbitrary code execution. Successful exploitation could give an attacker complete control of the affected system.

Oracle addressed CVE-2025-61757 in its October 2025 security update, confirming the issue as a high-impact, easily exploitable vulnerability requiring no authentication.

According to Searchlight Cyber, attackers leveraging this flaw could manipulate authentication workflows, escalate privileges, and pivot laterally into core infrastructure systems, putting servers handling user credentials and PII at substantial risk.

Following Thursday's public disclosure of technical details and proof-of-concept (PoC) exploit code, the SANS Technology Institute examined its honeypot telemetry to assess whether the vulnerability had already been targeted in the wild.

Recent 7-Zip Vulnerability Under Active Exploitation

A recently patched 7-Zip vulnerability, CVE-2025-11001 (CVSS 7.0), is now being exploited in real-world attacks. The issue involves a directory traversal flaw triggered during ZIP file parsing and relies on user interaction.

The vulnerability stems from improper handling of symbolic links within ZIP archives, allowing crafted archive contents to cause the extraction process to traverse outside intended directories.

According to a Trend Micro Zero Day Initiative advisory, attackers can exploit this flaw to execute code under the context of a service account, with the attack vector varying by deployment scenario.

The vulnerability, along with a related issue (CVE-2025-11002), was discovered by Ryota Shiga of GMO Flatt Security and reported to 7-Zip developers in May. Both were fixed in 7-Zip version 25.00, released in July.

NHS England has now issued a warning that threat actors are actively attacking unpatched 7-Zip installations.

The agency notes that a publicly available PoC enables attackers to abuse symbolic-link handling to place files outside the expected extraction directory—an action that, in some scenarios, can lead to RCE.

Security researcher Dominik C. further observed that the flaw affects how 7-Zip versions 21.02 through 24.09 convert Linux symbolic links into Windows paths, meaning the vulnerability is exploitable only on Windows systems.

UNC2891 Money Mule Network Exposes Full Extent of ATM Fraud Scheme

Cybersecurity researchers have mapped out the full breadth of a long-running ATM fraud campaign attributed to UNC2891, targeting two major Indonesian banks.

While the group's Raspberry Pi-based ATM intrusion documented in early July drew initial attention, a new investigation by Group-IB reveals a significantly larger criminal ecosystem built around recruiting money mules, generating cloned payment cards, and orchestrating coordinated ATM cash-out operations.

The report details three confirmed intrusions:

- Bank A – February 2022
- Bank B – November 2023
- Bank A – July 2024

In each case, UNC2891 deployed payloads packaged with its STEELCORGI toolset.

Group-IB's analysis shows the threat actors advertised mule recruitment posts on Google and Telegram, providing recruits with cloned-card tools shipped via postal services. Money mules then executed ATM withdrawals while being guided through real-time TeamViewer sessions or phone-based instructions.

The findings underscore that UNC2891's operations expanded far beyond technical compromise, incorporating a large-scale financial extraction and mule coordination network.

Broadcom Reportedly Targeted by Clop Ransomware Through Oracle E-Business Suite Zero-Day

The ClOp ransomware group claims to have breached internal systems at Broadcom through exploitation of an Oracle E-Business Suite zero-day, CVE-2025-61882.

Rated 9.8 (critical) on the CVSS scale, the vulnerability enables unauthenticated arbitrary code execution, allowing attackers to gain privileged access to enterprise environments.

Broadcom—one of the world's largest semiconductor and infrastructure software providers—is the latest organization affected in a widespread exploitation wave that began in late September 2025, targeting companies running unpatched Oracle E-Business Suite deployments.

Browser Push Notifications Weaponized to Deliver Malicious URLs

Threat actors are abusing browser notification features to deliver malicious links through a newly emerged cybercrime service known as Matrix Push C2, according to a Thursday report from BlackFog.

Browser notifications can appear as desktop alerts and may impersonate system dialogues or trusted applications. Matrix Push C2 offers an attacker-friendly interface enabling users to forge these notifications, complete with templates mimicking brands such as PayPal and Cloudflare.

Attackers must first social-engineer targets into granting push-notification permissions. Once approved, notifications can direct victims to malware or phishing pages.

One observed example involved a forged Chrome alert claiming an urgent update was required to prevent data loss, subsequently redirecting the victim to a site distributing a trojanized Chrome

installer.

Matrix Push C2 includes a dashboard that allows operators to customize branding, logos, links, and messaging—effectively functioning as a malicious push-notification marketing platform, BlackFog said.

Recent High to Critical CVEs

CVE-2025-65108 – md-to-pdf RCE Vulnerability

The md-to-pdf CLI utility, which converts Markdown files to PDF using Node.js and headless Chrome, contains an RCE flaw prior to version 5.2.5. When a Markdown file includes a front-matter block with a JavaScript delimiter, the gray-matter parsing engine may execute arbitrary code during processing. The issue is resolved in 5.2.5.

CVE-2025-65946 – Roo Code Improper Command Validation

Roo Code, an AI-assisted autonomous coding agent, improperly validated command prefixes prior to version 3.26.7, allowing execution of commands outside the approved allowlist. The flaw has been fixed in 3.26.7.

CVE-2025-65947 – thread-amount Resource Leak on Windows & macOS

The thread-amount utility leaked system resources before version 0.2.2.

On Windows, CreateToolhelp32Snapshot handles were not closed, causing handle exhaustion. On macOS, memory allocated by task_threads was not released, resulting in memory leaks and possible OOM termination.

Both issues are corrected in 0.2.2.

CVE-2025-13384 – CP Contact Form with PayPal Missing Authorization

All versions up to 1.3.56 of the WordPress CP Contact Form with PayPal plugin expose an unauthenticated endpoint (cp_contactformpp_ipncheck) that processes payment confirmations without any form of authentication. Attackers can forge payment notifications to falsely mark transactions as paid.

CVE-2025-13526 – OneClick Chat to Order IDOR Vulnerability

The WordPress OneClick Chat to Order plugin, up to version 1.0.8, lacks proper validation in the wa_order_thank_you_override function. This allows unauthenticated users to manipulate order IDs to access sensitive customer information, including personal details, addresses, order contents, and payment data.

Writer - [JoshAllen](#)

-1-

Spoiler ([Click to View](#))

-2-

Spoiler ([Click to View](#))

-3-

Spoiler ([Click to View](#))

-4-

Spoiler ([Click to View](#))

Spoiler [\(Click to View\)](#)

[Mix](#) [Cap](#) [Chrome](#) [MadScientist](#) [Oh_Well](#) [????????????](#) [JoshAllen](#)

If you have enjoyed the read please consider using one of our signatures in any way to support us!

Mooooookie - November 24, 2025, 12:41 pm
Thanks for compiling and sharing another edition of the HF News with us. Interesting read as usual.

Terry A. Davis - November 24, 2025, 12:47 pm

What is the criteria for being mentioned in honorable threads? Not really after anything. Just curious since I remember there used to be a sticky in the section that would let members nominate.

Tyr - November 24, 2025, 2:16 pm

Thanks for your time and dedication to those who helped. Also hey, thanks for the shoutout!

Jamika - November 24, 2025, 2:20 pm

Nlce work as usual and funny comics

padrino - November 24, 2025, 5:07 pm

Another great edition of HF News. Thanks for the great read!

6 - November 24, 2025, 10:45 pm

Good edition, i like the CVE section this week and also more hacker news.

Mix - November 25, 2025, 10:22 am

(Nov 24, 2025 01:47 PM)Depressed Wrote: [\[CITE\]](#) What is the criteria for being mentioned in honorable threads? Not really after anything. Just curious since I remember there used to be a sticky in the section that would let members nominate.

Right now we have the pinned thread in site news

<https://hackforums.net/showthread.php?tid=6299864> for user submissions. Noteable threads are picked by the team for threads that seem worthy, and the music section is from a few mixed threads spread from the music lounge all the way to the team's submissions. Headlines is mainly for bigger things like site changes or events happening on site. For example, the HF wiki is returning this week. I must admit I have been lacking grabbing user news each week currently due to time but I can say if we can get more people to submit changes or goals/milestones for users then I am sure Ill be able to add that section back weekly.

Terry A. Davis - November 25, 2025, 11:44 am

(Nov 25, 2025 11:22 AM)Mix Wrote: [\[CITE\]](#) Right now we have the pinned thread in site news <https://hackforums.net/showthread.php?tid=6299864> for user submissions. Noteable threads are picked by the team for threads that seem worthy, and the music section is from a few mixed threads spread from the music lounge all the way to the team's submissions. Headlines is mainly for bigger things like site changes or events happening on site. For example, the HF wiki is returning this week. I must admit I have been lacking grabbing user news each week currently due to time but I can say if we can get more people to submit changes or goals/milestones for users then I am sure Ill be able to add that section back weekly.

I either must be blind from cronic wanking, or I just didn't look that hard.

Ignore me then apparently I just didn't look hard enough or glossed over it in my infinite wisdom of how I read

RangoWorld - November 25, 2025, 11:18 pm

Thank you for yet another edition of HF News.