

Forum:[Hack Forums](#)

Thread: [Hack Forum News - Edition 20](#)

Mix - October 27, 2025, 10:44 am

Hack Forum News - Edition 20

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](#)

[OctoberFest 2025](#) By [Omniscient](#)

Octoberfest is now in the final days! We have seen a massive increase of activity across the site and, with the event, [Omniscient](#) has announced a giveaway that includes over \$2000 worth of prizes to be won. And the award for this year's event has been released, and a few members have already managed to get it twice. If you haven't seen this yet, then it's worth checking out and seeing what prizes are up for grabs this year, and you might even get lucky and get yourself a free \$500.

[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.

[HFX 3.0 - The BEST Browser Extension for Hack Forums](#) By [xadamxk](#)

Have you had that feeling that you have used HFX in the past, but due to browsers no longer using Manifesto v2, they have broken the extensions? Well, worry no more. [xadamxk](#) has remade the extension from scratch, and updated it to support modern browsers. With the new version of HFX, they have also packed in a load of new features for everyone to take advantage of. Make sure to check this thread for a few more details about what is included and to see if those features could be useful for someone like you.

Writer - [Mix](#)

Last Week:

Spoiler ([Click to View](#))

Writer - [Mix](#)

[jBarrel](#) Has obtained the "King Decade" award -
[TTxd3_T9](#) Has obtained the "King Decade" award -
[SIM-1895736](#) Has obtained the "King Decade" award -
[Kansur](#) Has obtained the "King Decade" award -
[Thron](#) Has obtained the "King Decade" award -
[Jovis](#) Has obtained the "King Decade" award -
[?ystem](#) Has obtained the "Green Apple" award -
[DAL-SHA](#) Has obtained the "Stanley Fan" award -
[Hackers](#) Has obtained the "Stanley Fan" award -
[RangoWorld](#) Has obtained the "Octoberfest 2025" award -
[Oh_Well](#) Has obtained the "Octoberfest 2025" award -
[sharn](#) Has obtained the "Octoberfest 2025" award -
[Mix](#) Has obtained the "Octoberfest 2025" award -
[Eran](#) Has obtained the "Octoberfest 2025" award -
[Aeowulf](#) Has obtained the "Octoberfest 2025" award -
[jcole](#) Has obtained the "Octoberfest 2025" award -
[Michael](#) Has obtained the "Octoberfest 2025" award -
[Palestine](#) Has obtained the "Octoberfest 2025" award -
[DAL-SHA](#) Has obtained the "Octoberfest 2025" award -
[onlineuser | D3RFER](#) Has obtained the "Octoberfest 2025" award -
[Charlie Sheen](#) Has obtained the "Octoberfest 2025" award -
[Yin Yang](#) Has obtained the "Octoberfest 2025" award -

Writer - [Oh_Well](#)

[Its offically my birthday!](#) - by [Mix](#)

The man behind HF News, [Mix](#) himself, celebrates another year around the sun! Unsure of how to mark the occasion, he asked the community for ideas. It's a fun reminder that without Mix, Notables and HF News probably wouldn't be a thing again. Be sure to wish him a happy birthday if you haven't already!

[Final week of Octoberfest](#) - by [Oh_Well](#)

The clock is ticking, we in the last week of Octoberfest! A discussion for the final push toward earning the event's award. If you've been procrastinating, now's the time to join the fun and finish strong before the month ends.

[All members who earned Octoberfest 2025 award so far](#) - by [Pimping](#)

[Pimping](#) keeps the Octoberfest spirit alive with a running list of everyone who's earned the 2025 Pumpkin award so far. The thread highlights 19 members, all grinding their way through the event. A

great way to track progress, cheer on your friends, and maybe get inspired to grab the badge yourself before the 31st.

[Thoughts on 3I/Atlas ??](#) - by [Chorozon](#)

Speculation meets curiosity in this thread about 3I/Atlas - humanity's third interstellar object. With a NASA blackout keeping details scarce, members can't help but wonder: is it a comet, an alien craft, or something else? Just another day on HF where science and conspiracy blend perfectly for a fun debate.

[Custom Build: Building a NAS, what hard drive to choose?](#) - by [HerrWinston](#)

[HerrWinston](#) is diving into a new DIY project — building his own NAS. He's after affordable 5TB drives, one for data and one for backup, and turns to the community for recommendations. With over a dozen replies, the thread quickly turns into a practical discussion on home storage setups.

[Warp.dev - Made a mini game in under 1 minute // 1 prompt](#) - by [Hackers](#)

[Hackers](#) puts Warp.dev to the test and ends up creating a mini game in under a minute - with just one prompt. He walks readers through his first impressions of the tool and shares screenshots and a demo video. Whether you're into AI-assisted coding or just curious about the hype, this thread is a cool glimpse into where developer workflows are headed.

[Do It Yourself: What tools, gadgets should I get aswell?](#) - by [HerrWinston](#)

[HerrWinston](#) returns with another hardware-focused thread, this time planning his 2025 gadget lineup. From Raspberry Pis and Arduinos to possibly a Flipper Zero, he's on a mission to level up his DIY skills. The community's chiming in with gear suggestions - a great thread for anyone wanting to dive deeper into electronics, tinkering, and home projects.

Writer - [Chrome](#)

GROUPS FOR SALE AND SOLD

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

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

Casino has been sold to [NERO](#)

RECENT GROUP CHANGES & EVENTS

No reported changes this week.

RECRUITMENTS:

[Casino Recruitment](#)
[Pink LSZ Recruitment](#)
[Warriors Recruitment](#)

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

Writer - [Mix](#)

[Moooookie](#) has reached 5,000 posts.

[DemonAsylum](#) has reached 5,000 excellent credibility. (Well done on being the first to achieve this.)

Remember if you have reached an achievement on your account feel free to post about it on our weekly reports thread. That way we can add you to the news for the next edition. [Click Here To See The Weekly Reports Thread](#)

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://www.youtube.com/watch?v=cI0wUoCLnLk>]

Writer - [Chrome](#)

[\\$100 Crypto Contest - Celebrating my entrance to Quantum](#) By [Oh_Well](#)

A new contest has been created this week by [Oh_Well](#) He is celebrating his entrance to the new group Quantum by giving away \$100. Make sure to enter!

[? Win the Handgun Award for Just \\$30 – FPS Video Challenge](#) by [7](#)

Well, this is an interesting one. Not necessarily a giveaway but an opportunity to win the ability to

purchase a custom award for just \$30. To enter you need to create a video of you playing an FPS game. More information click the link!

[MAXIMUM SECURITY UPLOAD - Can you HACK IT? \\$20 XMR](#) by [Rsynced](#)

Another cool challenge giveaway thread! The rules are simple, hack the website OP created using AI and provide proof then claim your \$20!

Mix - October 27, 2025, 10:52 am

Writer - [MadScientist](#)

Hackforums News Cybersecurity Vulnerabilities and News Digest

Mass exploitation campaign targets outdated WordPress plugins

A wide-scale campaign is actively targeting WordPress sites that still run outdated versions of the GutenKit and Hunk Companion plugins. The flaws—all of which are rated critical—can be chained to enable remote code execution (RCE) by allowing attackers to install additional plugins without proper authorization.

WordPress security vendor Wordfence reported blocking roughly 8.7 million attack attempts aimed at its customers during a concentrated two-day window (October 8–9).

The operation leverages three distinct vulnerabilities tracked as CVE-2024-9234, CVE-2024-9707, and CVE-2024-11972, each carrying a CVSS score of 9.8.

CVE-2024-9234 is an unauthenticated flaw in a REST endpoint of the GutenKit plugin (?40k installs) that permits installing arbitrary plugins without credentials.

CVE-2024-9707 and CVE-2024-11972 are missing-authorization issues in the themehunk-import REST endpoint of the Hunk Companion plugin (?8k installs) that likewise allow arbitrary plugin installation.

An attacker who can exploit these weaknesses (or chain them with other privileges) may introduce an additional backdoored plugin that grants remote code execution on the host.

Affected versions / fixes: CVE-2024-9234 impacts GutenKit <= 2.1.0. CVE-2024-9707 affects Hunk Companion <= 1.8.4; CVE-2024-11972 affects Hunk Companion <= 1.8.5. Patches were released (GutenKit 2.1.1 in Oct 2024; Hunk Companion 1.9.0 in Dec 2024), but many sites remain unpatched.

Source: BleepingComputer.

Emergency Windows Server updates fix WSUS RCE with public PoC

Microsoft pushed out-of-band updates to remediate a critical RCE vulnerability in Windows Server Update Services (WSUS), after proof-of-concept exploit code became public.

WSUS, the on-premises update-management component, is only vulnerable when the WSUS Server Role is enabled (it is not enabled by default).

Tracked as CVE-2025-59287, the flaw enables remote, unauthenticated attackers to trigger unsafe object deserialization in a legacy serialization path, resulting in code execution as SYSTEM. The attack vector is low complexity and requires no user interaction, raising wormability concerns between WSUS instances.

Microsoft emphasized that servers without the WSUS role are not affected, and that enabling the role without applying the fix will expose the host.

Microsoft published updates for all impacted Windows Server releases and urged immediate installation, including (selection): Windows Server 2025 (KB5070881), 23H2 (KB5070879), 2022 (KB5070884), 2019 (KB5070883), 2016 (KB5070882), 2012 R2 (KB5070886), and 2012 (KB5070887).

Source: BleepingComputer.

Former cyber exec charged over sale of secrets to Russia

U.S. federal prosecutors have indicted a former general manager in the cyber division of defense contractor L3Harris (Trenchant) on allegations of selling trade secrets to a buyer in the Russian Federation for roughly \$1.3 million.

The indictment states the defendant, Peter Williams, stole seven trade secrets belonging to two unnamed companies between April 2022 and June 2025 and knowingly intended them for sale outside the United States.

Court filings do not detail the exact nature of the secrets. Williams held senior roles at Trenchant, a unit involved in developing offensive cyber capabilities.

Source: The Register.

Microsoft blocks downloaded file previews to prevent NTLM hash leaks

As part of October 2025 Patch Tuesday, Microsoft disabled preview rendering for files marked with the Mark of the Web (MotW), a Windows flag applied to files downloaded via browsers or received as attachments.

MotW signals potentially unsafe content and already restricts risky behaviors (for example, disabling macros in Office documents). The new change prevents previewing such files, mitigating a flaw that could leak NTLM hashes during preview operations. Exfiltrated NTLM hashes can be brute-forced to recover credentials or abused in relay attacks.

Source: Microsoft advisory / reporting.

RedTiger — open-source Python red-team tool observed in the wild targeting gamers and Discord

RedTiger is an open-source Python red-team toolkit released in 2024 that bundles reconnaissance, network scanning, phishing toolkits, a Discord-focused module, and an infostealer. While intended for red-team and security research use, components have been observed reused by malicious actors.

Recent telemetry highlights multiple RedTiger-derived payloads in circulation, with the infostealer component specifically targeting gaming communities and Discord accounts—an active trend described in multiple analysis posts this month.

Source: Netskope blog.

AI misclassification leads to armed handcuffing of teenager in U.S. school incident

A Baltimore teenager was detained by heavily armed police after an AI system mistakenly flagged a crisps packet as a firearm. The student, 16-year-old Taki Allen, said officers arrived in force and ordered him onto the ground.

Baltimore County Police stated officers responded proportionally based on the information they were given. According to reports, human reviewers had dismissed the AI alert, but a school principal did not see the cleared alert and escalated the situation to the safety team, which called police.

The incident has renewed calls for reviewing procedures around AI-driven monitoring at schools. The student reported he had an empty Doritos packet in his pocket after football practice; police arrived approximately 20 minutes later.

Source: BBC.

MuddyWater (Iranian actor) deploys Phoenix backdoor against >100 government targets

The threat actor known as MuddyWater (aliases: Static Kitten, Mercury, Seedworm) executed a phishing campaign beginning August 19 that deployed Phoenix backdoor v4 across more than 100 government and diplomatic entities, primarily in the Middle East and North Africa.

Researchers from Group-IB report the campaign used a compromised [censored] account to originate phishing emails. On August 24 the attacker apparently disabled its server-side C2 component—suggesting a shift to alternate tooling or a new stage of operations. Most observed targets were embassies, foreign affairs ministries, consulates, and similar diplomatic missions.

Source: BleepingComputer.

This week's notable critical CVEs and POCs

CVE-2025-24813 — Apache Tomcat path equivalence / partial PUT RCE (PoC repos updated this week)

A path-equivalence / partial-PUT handling issue in Apache Tomcat that lets an attacker write or replace files (including uploading crafted serialized data) leading to unsafe deserialization and RCE under certain configurations. Several PoC repositories and exploit scripts have been published or refreshed recently.

CVE-2025-30208 — Vite dev server /@fs/ arbitrary file read (PoC scripts available)

A path traversal / @fs bypass in Vite dev server that allows arbitrary file reads via crafted query strings (e.g., ?raw?? trick). Several PoC exploit scripts and detection tools have been published to GitHub this week.

CVE-2025-24354 — imgproxy SSRF / OOB SSRF detections (PoC / Nuclei template added this week)

An image-proxy SSRF that allows internal network interaction (e.g., requests to 0.0.0.0) via crafted image retrieval paths. This week a community PoC and a Nuclei detection template were added to

project repos.

CVE-2025-62713 — Kottster (self-hosted Node.js admin panel): pre-auth RCE in development mode for versions 3.2.0 -> <3.3.2; fixed in 3.3.2. Production deployments were not affected.

CVE-2025-50951 — FontForge v20230101: memory leak via utf7toutf8_copy in /fontforge/sfd.c.

CVE-2025-58428 — TLS4B ATG SOAP interface: authenticated attackers can execute system-level commands on Linux hosts via accessible web services.

CVE-2025-12100 — MongoDB BI Connector ODBC driver: incorrect default permissions enable privilege escalation (affects 1.0.0 -> 1.4.6).

CVE-2025-59503 — Azure Compute Gallery: SSRF vulnerability allowing authorized attackers to escalate privileges over a network.

CVE-2025-60023 / CVE-2025-59776 / CVE-2025-62688 / CVE-2025-58429 / CVE-2025-62498 / CVE-2025-61934 — Multiple critical path-traversal, ZipSlip, and incorrect permission issues in "Productivity Suite" v4.4.1.19 permitting unauthenticated file/directory deletion, creation, arbitrary code execution, and privilege changes via the PLC simulator and related services.

CVE-2025-7730 — Bold Page Builder (WordPress): stored XSS via the percentage parameter in versions <= 5.4.5 allowing authenticated contributors and above to inject scripts that execute when pages are loaded.

Writer - [???????????](#)

Cybersecurity and Infrastructure Security Agency (CISA) warns of high-severity Windows SMB flaw now exploited in the wild

CISA has issued an alert for a critical vulnerability in Microsoft's SMB protocol (CVE-2025-33073, CVSS 8.8), affecting older Windows 10, Windows 11 and Windows Server versions. The flaw is being actively exploited, and users who haven't installed the June 2025 Patch or later are at heightened risk.

[Source](#)

Hackers exploiting critical vulnerability in Windows Server Update Service (WSUS) under active attacks

A serious code-execution bug (CVE-2025-59287) in Microsoft's WSUS platform is under active exploitation. Attackers have targeted multiple networks using the flaw; Microsoft issued an out-of-band update and urged urgent remediation. CISA added this flaw to its Known Exploited Vulnerabilities list.

[Source](#)

Jaguar Land Rover hack estimated to cost UK economy £1.9 billion, experts say

The cyberattack on Jaguar Land Rover is now estimated to have caused around £1.9 billion in damage across the UK economy, possibly making it the most costly cyber incident in British history. The supply-chain ripple effect impacted thousands of suppliers and smaller businesses.

[Source](#)

Breaking OT & IT silos: asset owners, vendors and agencies brace for industrial cybersecurity shift

Industry stakeholders are pivoting towards integrated IT/OT cyber-defence models. The article highlights persistent vendor lock-in, trust deficits and regulatory complexity that hamper information sharing in industrial control systems.

[Source](#)

Microsoft's 2025 report: AI & cyber-attacks blur boundaries between crime, espionage and disruption

A new report from Microsoft reveals how adversaries are increasingly leveraging AI to automate operations, speed attacks, and blur lines between traditional cyber-crime, espionage and disruption. Strategy needs to evolve accordingly.

[Source](#)

Writer - [Mix](#)

-1-
Spoiler [\(Click to View\)](#)

-2-
Spoiler [\(Click to View\)](#)

-3-
Spoiler [\(Click to View\)](#)

-4-
Spoiler [\(Click to View\)](#)

-5-
Spoiler [\(Click to View\)](#)

A big thank you to all the members who put in the hard work to bring us another edition of HF News this week

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

Support The Team by wearing our signatures

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

Red
Code
[align=center][url=https://hackforums.net/forumdisplay.php?fid=2][img]https://hackforums.net/images/hfnews/support-red.png[/img][/url]/[align]
Blue
Code
[align=center][url=https://hackforums.net/forumdisplay.php?fid=2][img]https://hackforums.net/images

/hfnews/support-gray.png[/img][url][align]

Green

Code

[align=center][url=https://hackforums.net/forumdisplay.php?fid=2][img]https://hackforums.net/images/hfnews/support-magenta.png[/img][url][align]

Orange

Code

[align=center][url=https://hackforums.net/forumdisplay.php?fid=2][img]https://hackforums.net/images/hfnews/support-brown.png[/img][url][align]

Purple

Code

[align=center][url=https://hackforums.net/forumdisplay.php?fid=2][img]https://hackforums.net/images/hfnews/support-magenta-2.png[/img][url][align]

Jinu - October 27, 2025, 10:59 am

Thank you for this wonderful news in simple and clear way of presentation. It is very easy to know what is happening in the forum.

Palestine - October 27, 2025, 11:01 am

Awesome I love these HF news it's very informative and interesting great work ??

Jamika - October 27, 2025, 11:18 am

Good work bro , but excuse me

- 1- video not working (say not available in your country, damn)
- 2- where is my 10k posts ? will report u to omni (jk)

Mememes are hilarious ???

Mix - October 27, 2025, 11:20 am

(Oct 27, 2025 11:18 AM)Jamika Wrote: [CITE](#) Good work bro , but excuse me

- 1- video not working (say not available in your country, damn)
- 2- where is my 10k posts ? will report u to omni (jk)

Mememes are hilarious ???

Your 10k posts was mentioned in last weeks edition.

I might see if I can find another version of it if thats the case for others.

Hackers - October 27, 2025, 12:23 pm

o.O technically I'm in here 3 times because I put the Hozier video up :O

Nice news breakdown.

I hope people check out Warp.dev, I haven't paid a penny yet and I had some really good MVPs from there.

I also made this with Warp:

<https://hackforums.net/showthread.php?tid=6312236>

++ a similar tool but with normal .sh shell script

& a full PHP Admin dashboard with 10+ modules supported (other PHP repos, packaged into 1

central dash)

& a few other prototypes too.

Very surprised, Warp knocked it out of the park for being free. Not a huge fan of their UI but they have auto-approve commands whitelists, multi-file AI agents, etc... Hard to be upset at a UI issue (i don't like how they make you swap to terminal mode).

JoshAllen - October 27, 2025, 2:05 pm

Amazing edition as always! You have no idea how much I love reading these.

RangoWorld - October 27, 2025, 2:12 pm

Happy Birthday once again [Mix](#)

Appreciate all the good work here

CL1B - October 27, 2025, 4:38 pm

Thank you for this week's edition!

Aeowulf - October 27, 2025, 5:17 pm

As always, appreciate the effort that goes into this!

Pimping - October 27, 2025, 7:49 pm

Another great news thread

love reading these.... keep up the good work guys

xadamxk - October 27, 2025, 8:02 pm

Thanks for the HFX shoutout. Great work as always news team!

JoshAllen - October 29, 2025, 8:47 am

Have you considered adding a sports section?

Chrome - October 29, 2025, 12:45 pm

(Oct 29, 2025 08:47 AM)Josh Allen Wrote: [CITE](#) Have you considered adding a sports section?

We are happy to consider any section if we have the right person propose it to us and was happy to write the section.

The key is we need people to be able to consistently write each week. Our issue has been finding someone that's reliable enough.

So yes, for sure!

DemonAsylum - October 31, 2025, 10:18 pm

Another great edition as usual. It's been awesome seeing the statistics from all of the increased activity due to Octoberfest. That and of course everyone getting their pumpkin awards and a good amount of people getting their decade award too from checking on the Octoberfest award progress lol. Keep up the great work!