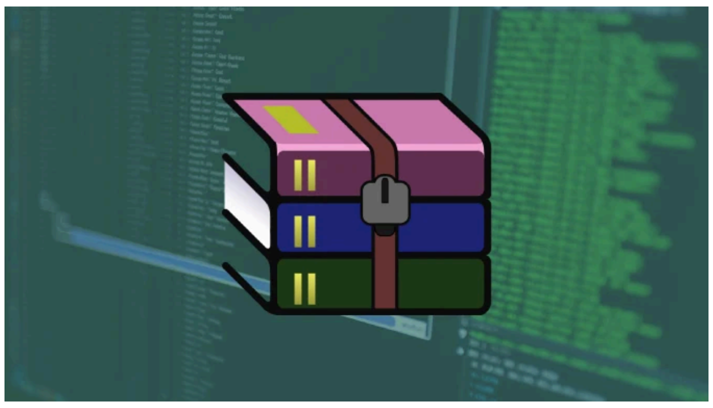
Week of August 11, 2025

Cybersecurity Headlines

Digital Threat Landscape

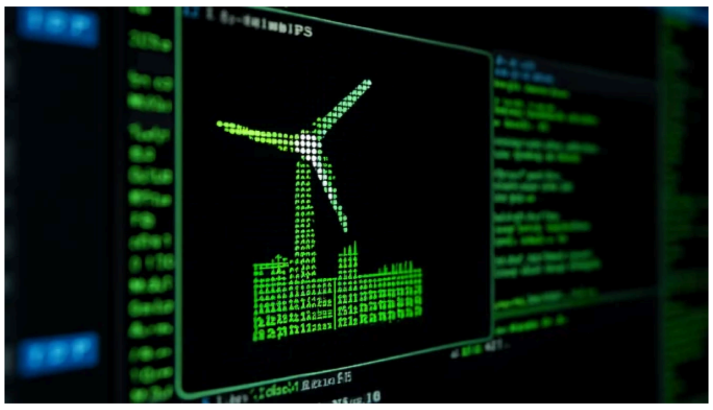
Cybercrimes, Scams, Threats, Vulnerabilities and Incidents



WinRAR Zero-Day Under Active Exploitation – Update to Latest Version Immediately

thehackernews.com

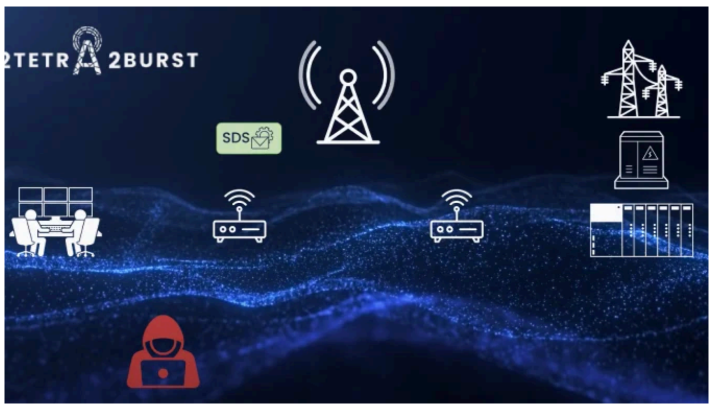
Tracked as CVE-2025-8088 (CVSS score: 8.8), the issue has been described as a case of path traversal affecting the Windows version of the tool that could be exploited to obtain arbitrary code execution by crafting malicious archive files.



Researchers Spot Surge in Erlang/OTP SSH RCE Exploits, 70% Target OT Firewalls - The Hacker News

thehackernews.com

Malicious actors have been observed exploiting a now-patched critical security flaw impacting Erlang/Open Telecom Platform (OTP) SSH as early as beginning of May 2025, with about 70% of detections originating from firewalls protecting operational tec...



New TETRA Radio Encryption Flaws Expose Law Enforcement Communications - The Hacker News

thehackernews.com

The newly discovered issues relate to a case of packet injection in TETRA, as well as an insufficient fix for CVE-2022-24401, one of the five flaws that was documented as part of TETRA:BURST, to prevent keystream recovery attacks. The identified vuln...

Industry Updates

Legislation, Business, Privacy, Updates, Related Technologies

GitHub will join Microsoft's CoreAI division with departure of CEO Thomas Dohmke

www.geekwire.com

Microsoft will bring GitHub into its CoreAI division with the announcement this morning that GitHub CEO Thomas Dohmke will be stepping down as the leader of the widely used software development platform and code repository.

Microsoft Patch Tuesday, August 2025 Edition

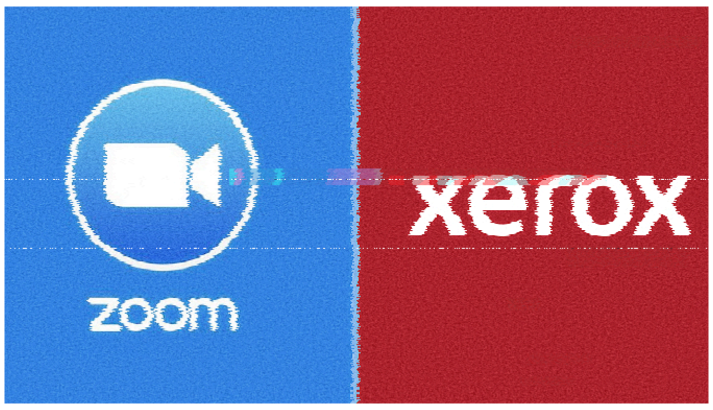
krebsonsecurity.com

Microsoft today released updates to fix more than 100 security flaws in its Windows operating systems and other software. At least 13 of the bugs received Microsoft's most-dire "critical" rating, meaning they could be abused by malware or malcontents to gain remote access to a Windows system with little or no help from users.

Mobile Phishers Target Brokerage Accounts in 'Ramp and Dump' Cashout Scheme

krebsonsecurity.com

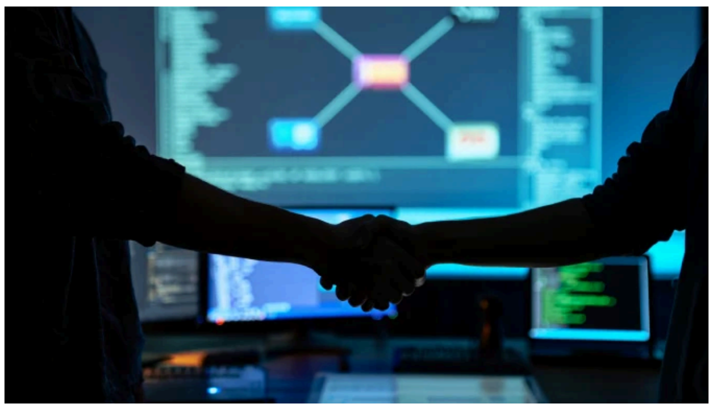
Mobile Phishers Target Brokerage Accounts in 'Ramp and Dump' Cashout Scheme



Zoom and Xerox Release Critical Security Updates Fixing Privilege Escalation and RCE Flaws - The Hacker News

thehackernews.com

Zoom and Xerox have addressed critical security flaws in Zoom Clients for Windows and FreeFlow Core that could allow privilege escalation and remote code execution. The vulnerability impacting Zoom Clients for Windows, tracked as CVE-2025-49457 (CVSS...



Cybercrime Groups ShinyHunters, Scattered Spider Join Forces in Extortion Attacks on Businesses - The Hacker News

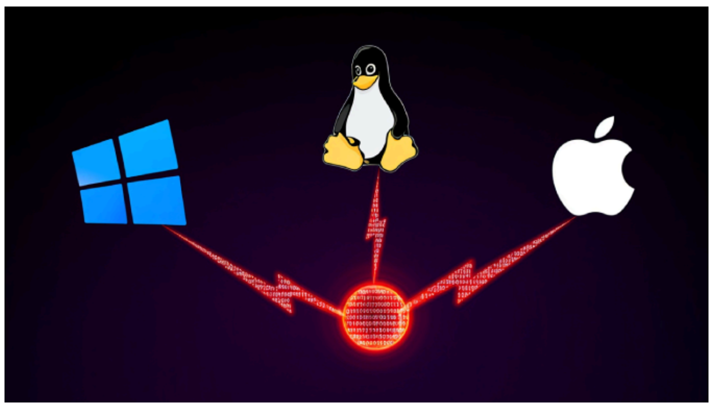
thehackernews.com

An ongoing data extortion campaign targeting Salesforce customers may soon turn its attention to financial services and technology service providers, as ShinyHunters and Scattered Spider appear to be working hand in hand, new findings show. "This lat...

DEF CON volunteers step up to help water sector after China, Iran attack utilities

therecord.media

When Jake Braun put out a call online last year seeking volunteers who wanted to help secure a water utility, the response was so overwhelming that he had to shut down the website.



Hackers Found Using CrossC2 to Expand Cobalt Strike Beacon's Reach to Linux and macOS

thehackernews.com

Japan's CERT coordination center (JPCERT/CC) on Thursday revealed it observed incidents that involved the use of a command-and-control (C2) framework called CrossC2, which is designed to extend the functionality of Cobalt Strike to other platforms like Linux and Apple macOS for cross-platform system control.

New York lawsuit against Zelle creator alleges features allowed $1 billion in thefts

therecord.media

The creator of the Zelle electronic payment platform is facing a lawsuit from the state of New York over accusations the company did little to stop scammers from using it to steal more than $1 billion from users between 2017 and 2023.

***Please be advised that** the following resources and materials are for informational purposes only. **The opinions and views expressed in these materials** are the opinions of the designated authors and do not reflect the opinions or views of **the Commonwealth of Massachusetts, the Executive Office of Technology Services and Security, and/or the Enterprise Risk Management Office, (the Commonwealth).** The information posted on this website includes hypertext links or pointers to information created and maintained by other public and/or private organizations. These links and pointers are provided solely for the information and convenience of the user. By selecting a link to an outside website, the user is subject to the privacy, copyright, security, and information quality policies of that website. The Commonwealth is not responsible for transmissions users receive from linked websites.*

External Quick links

- AIScoop
- BleepingComputer
- Cisco Talos Intelligence Group
- CSO Online
- CyberScoop
- Cybersecurity Dive
- Cyware
- CyberWire
- FedScoop
- Government Executive
- Government Technology
- ISACA
- ISSA International
- Krebs on Security
- MITRE ATT&CK®
- NASCIO
- Schneier on Security
- SC Media
- StateScoop
- The Hacker News
- The Record