Daily Intelligence Update | 12 November 2025

Researchers have identified four malicious npm packages published by an actor using the alias "flashbotts" that impersonate Flashbots and cryptographic utilities to harvest Web3 wallet credentials, private keys, and mnemonic seeds. The packages — ethers-provide-bundle, flashbot-sdk-eth, sdk-ethers, and gram-utilz — include a trojanized FlashbotsBundleProvider that exfiltrates environment variables and redirects unsigned transactions, a cryptographic utility that sends mnemonic phrases, a Flashbots client that steals keys on initialization, and a Telegram exfiltration utility forwarding secrets to bot ID 8083151136 (chat ID 5013747314). Analysts found the malicious routines padded with benign code and error suppression to evade detection, and noted targeting of MEV searchers, validators, and Web3 developers who manage hot wallets. At discovery the packages were live on npm and researchers have petitioned for removal while advising immediate package removal, key rotation, and supply-chain scanning to detect Telegram exfiltration or encoded secrets in dependencies.

CISA published a detailed technical analysis of malware used to exploit two zero-day flaws in Ivanti Endpoint Manager Mobile (EPMM), an authentication bypass tracked as CVE-2025-4427 and a code injection issue tracked as CVE-2025-4428. The vulnerabilities affected EPMM versions 11.12.0.4, 12.3.0.1, 12.4.0.1, and 12.5.0.0 and were patched on May 13, 2025, but evidence indicates limited targeted exploitation prior to the fixes. CISA's analysis describes two distinct malware sets delivered via segmented, Base64-encoded chunks over HTTP GET requests to the /mifs/rs/api/v2/ endpoint, employing loaders named web-install.jar along with malicious listeners that decode and execute arbitrary code. The reported toolset allowed reconnaissance, data theft, and persistence by intercepting and reconstructing payload fragments from HTTP traffic. CISA released IOCs, YARA signatures, and SIGMA rules to support detection and urged affected organizations to isolate impacted systems, collect forensic evidence, and apply patches immediately.

Researchers have identified a newly observed data leak site titled Kazu, which includes Ransom and Databases sections and has been promoted across cybercrime forums since April 2025. Kazu currently lists three ransom victims with demands in the USD 100,000 to 300,000 range and advertises databases for sale priced from USD 100 to 4,000, aggregating breaches primarily affecting government and public service portals across Asia, the Middle East, and Latin America. Separately, forum activity on October 31, 2025 surfaced a potential Knownsec leak advertised by a new user named "t1g3r" claiming thousands of files and tools tied to Chinese offensive cyber capabilities; researchers who downloaded sample screenshots found references to IP analysis tools, remote control functions, and maps of critical infrastructure, but cautioned that authenticity is unverified and Telegram chatter shows community skepticism. In related marketplace activity, an actor operating as "BreachParty" and previously "Colmenero" resurfaced in October 2025 selling Spain-focused datasets, reposting some stale material that matched confirmed 2023 leaks alongside other datasets that could not be validated; researchers advise treating these vendor claims with caution and validating samples before escalation.

Industrial control vendors continue to appear in high-impact advisories, with researchers disclosing critical vulnerabilities in Red Lion Sixnet SixTRAK and VersaTRAK RTUs allowing unauthenticated remote code execution and root-level command execution. The two tracked flaws, CVE-2023-40151 and CVE-2023-42770, are rated CVSS 10.0 and affect multiple models including ST-IPm-8460 and VT-IPm2m-213-D. One issue enables unauthenticated TCP access on port 1594 to bypass authentication while the other abuses the UDR Linux shell functionality to execute arbitrary commands. Red Lion released patches in June 2025 and recommended enabling authentication and blocking TCP access to reduce exposure, and CISA warned that exploitation could disrupt energy, water, transportation, and manufacturing systems.

Forum and underground chatter in October 2025 shows active interest in several disclosed vulnerabilities, with actors seeking working exploits for long-tail and recent flaws. Notable discussion includes requests for a working exploit for CVE-2024-38077 affecting Windows Remote Desktop Licensing Service, inquiries about usable PoCs for CVE-2025-49844 (a Redis Lua interpreter use-after-free allowing RCE for

authenticated users), and interest in CVE-2025-30247, an OS command injection in Western Digital My Cloud firmware. Posts also referenced offers to sell an unspecified zero-day corporate VPN RCE exploit, though pricing and details were exchanged privately. Researchers observed that some claimed PoCs on GitHub were pseudocode or unreliable, and actors complained about varying exploit quality, indicating an active but noisy market for weaponization. Defenders should prioritize known exploited and high-impact flaws, monitor exploit chatter, and validate indicators before actioning vendor claims.
