A FEDERAL CYBER CENTER

DoD CYBER CRIME CENTER (DC3)

DoD—Defense Industrial Base Collaborative Information Sharing Environment

24 Feb 25

Cyber Threat Roundup

A collection of recent open-source items of interest to the Defense Industrial Base

Contents

Articles

CISA Flags Craft CMS Vulnerability CVE-2025-23209 Amid Active Attacks

A high-severity security flaw impacting the Craft content management system (CMS) has been added by the U.S. Cybersecurity and Infrastructure Security Agency (CISA) to its Known Exploited Vulnerabilities (KEV) catalog, based on evidence of active exploitation. The vulnerability in question is CVE-2025-23209 (CVSS score: 8.1), which impacts Craft CMS versions 4 and 5. It was addressed by the project maintainers in late December 2024 in versions 4.13.8 and 5.5.8. "Craft CMS contains a code injection vulnerability that allows for remote code execution as vulnerable versions have compromised user security keys," the agency said.

https://thehackernews.com/2025/02/cisa-flags-craft-cms-vulnerability-cve.html

Cisco Confirms Salt Typhoon Exploited CVE-2018-0171 to Target US Telecom Networks

Cisco has confirmed that a Chinese threat actor known as Salt Typhoon gained access by likely abusing a known security flaw tracked as CVE-2018-0171, and by obtaining legitimate victim login credentials as part of a targeted campaign aimed at major U.S. telecommunications companies. The threat actor then demonstrated their ability to persist in target environments across equipment from multiple vendors for extended periods, maintaining access in one instance for over three years. "In addition, we have observed the threat actor capturing SNMP, TACACS, and RADIUS traffic, including the secret keys used between network devices and TACACS/RADIUS servers," Talos noted. "The intent of this traffic capture is almost certainly to enumerate additional credential details for follow-on use."

https://thehackernews.com/2025/02/cisco-confirms-salt-typhoon-exploited.html

Atlassian Fixed Critical Flaws in Confluence and Crowd

On 18 Feb 25, software firm Atlassian released security patches to address 12 critical- and high-severity vulnerabilities in Bamboo, Bitbucket, Confluence, Crowd, and Jira products. Multiple critical vulnerabilities in Apache Tomcat are addressed, some with a CVSS score of 9.8, allow for remote code execution (RCE) and authentication bypass. Updating to the latest versions of Tomcat (9.0.99, 10.1.35, or 11.0.3) is crucial to mitigate these threats, especially for users with case-insensitive file systems.

https://securityaffairs.com/174474/security/atlassian-fixed-critical-flaws-in-confluence-and-crowd.html

Cybercriminals Can Now Clone Any Brand's Site in Minutes Using Darcula PhaaS v3

The threat actors behind the Darcula phishing-as-a-service (PhaaS) platform appear to be readying a new version that allows prospective customers and cyber crooks to clone any brand's legitimate website and create a phishing version, further bringing down the technical expertise required to pull off phishing attacks at scale.
The cybersecurity company Netcraft said it has detected and blocked more than 95,000 new Darcula phishing domains, nearly 31,000 IP addresses, and taken down more than 20,000 fraudulent websites since it was first exposed in late March 2024.

https://thehackernews.com/2025/02/cybercriminals-can-now-clone-any-brands.html

Vulnerabilities in MongoDB Library Allow RCE on Node.js Servers

Two critical-severity vulnerabilities in the Mongoose Object Data Modeling (ODM) library for MongoDB could have allowed attackers to achieve remote code execution (RCE) on the Node.js application server, cybersecurity platform OPSWAT reports. Widely adopted in production environments, Mongoose enables the mapping of JavaScript objects to MongoDB documents, leading to easier data management and validation. However, the function that improves working with relationships between documents could be exploited for RCE. The cybersecurity organization has released proof-of-concept (PoC) exploit code targeting both vulnerabilities and recommends updating Mongoose to version 8.9.5 or later, which contain complete patches for the two bugs.

https://www.securityweek.com/vulnerabilities-in-mongodb-library-allow-rce-on-node-js-servers/

Beware: PayPal "New Address" Feature Abused to Send Phishing Emails

An ongoing PayPal email scam exploits the platform's address settings to send fake purchase notifications, tricking users into granting remote access to scammers. For the past month, BleepingComputer and others have received emails from PayPal stating, "You added a new address. This is just a quick confirmation that you added an address in your PayPal account." The email includes the new address that was allegedly added to your PayPal account, including a message claiming to be a purchase confirmation for a MacBook M4, and to call the enclosed PayPal number if you did not authorize the purchase. The emails are being sent directly by PayPal from the address "service@paypal.com," causing people to be concerned their account was hacked. Furthermore, as the emails are legitimate PayPal emails, they are bypassing security and spam filters.

https://www.bleepingcomputer.com/news/security/beware-paypal-new-address-feature-abused-to-send-phishing-emails/