Scottish Cyber Coordination Centre

Daily threat bulletin

9 September 2024

Vulnerabilities

Progress LoadMaster vulnerable to 10/10 severity RCE flaw

BleepingComputer - 08 September 2024 11:11

Progress Software has issued an emergency fix for a maximum (10/10) severity vulnerability impacting its LoadMaster and LoadMaster Multi-Tenant (MT) Hypervisor products that allows attackers to remotely execute commands on the device. [...]

SonicWall SSLVPN access control flaw is now exploited in attacks

BleepingComputer - 06 September 2024 10:20

SonicWall is warning that a recently fixed access control flaw tracked as CVE-2024-40766 in SonicOS is now “potentially” exploited in attacks, urging admins to apply patches as soon as possible. [...]

A flaw in WordPress LiteSpeed Cache Plugin allows account takeover

Security Affairs - 07 September 2024 12:13

A critical flaw in the LiteSpeed Cache plugin for WordPress could allow unauthenticated users to take control of arbitrary accounts. The LiteSpeed Cache plugin is a popular caching plugin for WordPress that accounts for over 5 million active installations. The plugin offers site acceleration through server-level caching and various optimization features. The LiteSpeed Cache plugin [...]

Apache fixed a new remote code execution flaw in Apache OFBiz

Security Affairs - 06 September 2024 09:13

Apache addressed a remote code execution vulnerability affecting the Apache OFBiz open-source enterprise resource planning (ERP) system. Apache fixed a high-severity vulnerability, tracked as CVE-2024-45195 (CVSS score: 7.5) affecting the Apache OFBiz open-source enterprise resource planning (ERP) system. Apache OFBiz® is an open source product for the automation of enterprise processes that includes framework components and business [...]

GeoServer Vulnerability Targeted by Hackers to Deliver Backdoors and Botnet Malware

The Hacker News - 06 September 2024 21:44

A recently disclosed security flaw in OSGeo GeoServer GeoTools has been exploited as part of multiple campaigns to deliver cryptocurrency miners, botnet malware such as Condi and JenX, and a known backdoor called SideWalk. The security vulnerability is a critical remote code execution bug (CVE-2024-36401, CVSS score: 9.8) that could allow malicious actors to take over susceptible instances.

Scottish Cyber Coordination Centre

GitHub Actions Vulnerable to Typosquatting, Exposing Developers to Hidden Malicious Code

The Hacker News - 06 September 2024 21:33

Threat actors have long leveraged typosquatting as a means to trick unsuspecting users into visiting malicious websites or downloading booby-trapped software and packages. These attacks typically involve registering domains or packages with names slightly altered from their legitimate counterparts (e.g., goog1e.com vs. google.com).

Veeam Patches Critical Vulnerabilities in Enterprise Products

SecurityWeek - 06 September 2024 11:52

Veeam has released patches for critical-severity vulnerabilities in Backup & Replication, ONE, and Service Provider Console. The post Veeam Patches Critical Vulnerabilities in Enterprise Products appeared first on SecurityWeek.

CISA Adds Three Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added three new vulnerabilities to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation: CVE-2021-20123 Draytek VigorConnect Path Traversal Vulnerability CVE-2021-20124; Draytek VigorConnect Path Traversal Vulnerability CVE-2024-7262; Kingsoft WPS Office Path Traversal Vulnerability.

Threat actors and malware

North Korean Threat Actors Deploy COVERTCATCH Malware via LinkedIn Job Scams

The Hacker News - 07 September 2024 13:58

Threat actors affiliated with North Korea have been observed leveraging LinkedIn as a way to target developers as part of a fake job recruiting operation. These attacks employ coding tests as a common initial infection vector, Google-owned Mandiant said in a new report about threats faced by the Web3 sector."

'TIDrone' Cyberattackers Target Taiwan's Drone Manufacturers

darkreading - 09 September 2024 02:00

The Chinese-speaking group is launching sophisticated malware towards military and satellite targets globally.

US and Allies Accuse Russian Military of Destructive Cyber-Attacks

Infosecurity Magazine - 06 September 2024 11:20

The joint government advisory highlighted the cyber activities of Unit 29155, which has launched destructive cyber-attacks against critical infrastructure globally.

Fog Ransomware Now Targeting the Financial Sector

Scottish Cyber Coordination Centre

Cyware News - Latest Cyber News - 07 September 2024 01:00

Fog, a variant of STOP/DJVU family, targets various sectors, exploiting VPN vulnerabilities to infiltrate network defenses. After infiltration, Fog ransomware disables protective measures, encrypts vital files, and demands ransom via the Tor network.

CyberVolk Ransomware: A New and Evolving Threat to Global Cybersecurity

Cyware News - Latest Cyber News - 07 September 2024 01:00

CyberVolk, infamous for DDoS attacks and data breaches, has gained particular notoriety for its ransomware, detected in July 2024, due to its advanced features and capabilities.

New RAMBO attack steals data using RAM in air-gapped computers

BleepingComputer - 07 September 2024 11:15

A novel side-channel attack dubbed "RAMBO" (Radiation of Air-gapped Memory Bus for Offense) generates electromagnetic radiation from a device's RAM to send data from air-gapped computers. [...]