Scottish Cyber Coordination Centre

Daily Threat Bulletin

11 June 2024

Vulnerabilities

Arm warns of actively exploited flaw in Mali GPU kernel drivers

BleepingComputer - 10 June 2024 19:53

Arm has issued a security bulletin warning of a memory-related vulnerability in Bifrost and Valhall GPU kernel drivers that is being exploited in the wild.

Netgear WNR614 flaws allow device takeover, no fix available

BleepingComputer - 10 June 2024 18:38

Researchers found half a dozen vulnerabilities of varying severity impacting Netgear WNR614 N300, a budget-friendly router that proved popular among home users and small businesses.

Exploit for critical Veeam auth bypass available, patch now

BleepingComputer - 10 June 2024 12:05

A proof-of-concept (PoC) exploit for a Veeam Backup Enterprise Manager authentication bypass flaw tracked as CVE-2024-29849 is now publicly available, making it urgent that admins apply the latest security updates.

Azure Service Tags Vulnerability: Microsoft Warns of Potential Abuse by Hackers

The Hacker News - 10 June 2024 17:50

Microsoft is warning about the potential abuse of Azure Service Tags by malicious actors to forge requests from a trusted service and get around firewall rules, thereby allowing them to gain unauthorized access to cloud resources.

Nvidia Patches High-Severity GPU Driver Vulnerabilities

SecurityWeek - 10 June 2024 12:40

Nvidia patches multiple high-severity vulnerabilities in GPU display drivers and virtual GPU software. The GPU driver updates, rolling out as versions R555, R550, R535, and R470, resolve a total of five security defects, three of which are rated ‘high severity’ and two rated ‘medium severity’.

Cisco Finds 15 Vulnerabilities in AutomationDirect PLCs

SecurityWeek - 10 June 2024 12:08

Cisco Talos researchers have found over a dozen vulnerabilities in AutomationDirect PLCs, including flaws that could be valuable to attackers.

Scottish Cyber Coordination Centre

Threat actors and malware

Gitloker attacks abuse GitHub notifications to push malicious oAuth apps

BleepingComputer - 10 June 2024 19:24

Threat actors impersonate GitHub's security and recruitment teams in phishing attacks to hijack repositories using malicious OAuth apps in an ongoing extortion campaign wiping compromised repository, among other things.

23andMe data breach under investigation in UK and Canada

BleepingComputer - 10 June 2024 12:00

Privacy authorities in Canada and the United Kingdom have launched a joint investigation to assess the scope of sensitive customer information exposed in last year's 23andMe data breach.

More_eggs Malware Disguised as Resumes Targets Recruiters in Phishing Attack

The Hacker News - 10 June 2024 21:54

Cybersecurity researchers have spotted a phishing attack distributing the More_eggs malware by masquerading it as a resume, a technique originally detected more than two years ago. The attack, which was unsuccessful, targeted an unnamed company in the industrial services industry in May 2024, Canadian cybersecurity firm eSentire disclosed last week.

CVE-2024-4577 quickly weaponized to distribute “TellYouThePass” Ransomware

Security Boulevard - 10 June 2024 19:05

Imperva Threat Research reported on attacker activity leveraging the new PHP vulnerability, CVE-2024-4577. From as early as June 8th, we have detected attacker activity leveraging this vulnerability to deliver malware, which we have now identified to be a part of the “TellYouThePass” ransomware campaign.

Snowflake Attacks: Mandiant Links Data Breaches to Infostealer Infections

SecurityWeek - 10 June 2024 17:08

Mandiant says a financially motivated threat actor has compromised hundreds of Snowflake instances using customer credentials stolen via infostealer malware that infected non-Snowflake owned systems.