Scottish Cyber Coordination Centre

Daily threat bulletin

4 September 2024

Vulnerabilities

Zyxel warns of critical OS command injection flaw in routers

BleepingComputer - 03 September 2024 16:59

Zyxel has released security updates to address a critical vulnerability impacting multiple models of its business routers, potentially allowing unauthenticated attackers to perform OS command injection. [...]

D-Link says it is not fixing four RCE flaws in DIR-846W routers

BleepingComputer - 03 September 2024 12:46

D-Link is warning that four remote code execution (RCE) flaws impacting all hardware and firmware versions of its DIR-846W router will not be fixed as the products are no longer supported. [...]

VMware fixed a code execution flaw in Fusion hypervisor

Security Affairs - 03 September 2024 22:22

VMware released a patch to address a high-severity code execution flaw in its Fusion hypervisor, users are urged to apply it. VMware addressed a high-severity code execution vulnerability, tracked as CVE-2024-38811 (CVSS 8.8/10), in its Fusion hypervisor. The vulnerability is due to the usage of an insecure environment variable, a threat actor with standard user privileges can [...]

New Flaws in Microsoft macOS Apps Could Allow Hackers to Gain Unrestricted Access

The Hacker News - 03 September 2024 10:31

Eight vulnerabilities have been uncovered in Microsoft applications for macOS that an adversary could exploit to gain elevated privileges or access sensitive data by circumventing the operating system's permissions-based model, which revolves around the Transparency, Consent, and Control (TCC) framework.

Chrome 128 Updates Patch High-Severity Vulnerabilities

SecurityWeek - 03 September 2024 08:46

Google has released two Chrome 128 updates to address six high-severity vulnerabilities reported by external researchers.

Threat actors and malware

Scottish Cyber Coordination Centre

Cyberattackers Spoof Palo Alto VPNs to Spread WikiLoader Variant

darkreading - 03 September 2024 19:25

The malware, first discovered two years ago, has returned in campaigns using SEO poisoning.

IT threat evolution Q2 2024

Securelist - 03 September 2024 09:00

In this report, Kaspersky researchers explore the most significant attacks of Q2 2024 that used a XZ backdoor, the LockBit builder, ShrinkLocker ransomware, etc.

UK related

Transport for London confirms cyberattack, assures us all is well

The Register - 03 September 2024 10:40

Government body claims there is no evidence of customer data being compromised
Transport for London (TfL) – responsible for much of the public network carrying people around England's capital – is battling to stay on top of an unfolding "cyber security incident".