Scottish Cyber Coordination Centre

Daily threat bulletin

3 May 2024

Vulnerabilities

Popular Android Apps Like Xiaomi, WPS Office Vulnerable to File Overwrite Flaw

The Hacker News - 02 May 2024 20:52

Several popular Android applications available in Google Play Store are susceptible to a path traversal-affiliated vulnerability codenamed the Dirty Stream attack that could be exploited by a malicious app to overwrite arbitrary files in the vulnerable app's home directory."The implications of this vulnerability pattern include arbitrary code execution and token theft,

New "Goldoon" Botnet Targets D-Link Routers With Decade-Old Flaw

The Hacker News - 02 May 2024 16:40

A never-before-seen botnet called Goldoon has been observed targeting D-Link routers with a nearly decade-old critical security flaw with the goal of using the compromised devices for further attacks.The vulnerability in question is CVE-2015-2051 (CVSS score: 9.8), which affects D-Link DIR-645 routers and allows remote attackers to execute arbitrary

CISA Warns of Active Exploitation of Severe GitLab Password Reset Vulnerability

The Hacker News - 02 May 2024 12:45

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has added a critical flaw impacting GitLab to its Known Exploited Vulnerabilities (KEV) catalog, owing to active exploitation in the wild.Tracked as CVE-2023-7028 (CVSS score: 10.0), the maximum severity vulnerability could facilitate account takeover by sending password reset emails to an unverified email

CISA and FBI Release Secure by Design Alert to Urge Manufacturers to Eliminate Directory Traversal Vulnerabilities

CISA Advisories -

Today, CISA and the Federal Bureau of Investigation (FBI) released a joint Secure by Design Alert, Eliminating Directory Traversal Vulnerabilities in Software. This Alert was crafted in response to recent well-publicized threat actor campaigns that exploited directory traversal vulnerabilities in software (e.g., CVE-2024-1708, CVE-2024-20345) to compromise users of the software—impacting critical infrastructure sectors, including the Healthcare and Public Health Sector.Additionally, this Alert highlights the prevalence, and continued threat actor exploitation of, directory traversal defects. Currently, CISA has listed 55 directory traversal vulnerabilities in our Known Exploited Vulnerabilities (KEV) catalog. Approaches to avoid directory traversal vulnerabilities are known, yet threat actors continue to exploit these vulnerabilities which have impacted the operation of critical services, including hospital and school operations.

Scottish Cyber Coordination Centre

Threat actors and malware

Microsoft Graph API Emerges as a Top Attacker Tool to Plot Data Theft

darkreading - 02 May 2024 11:00

Weaponizing Microsoft's own services for command-and-control is simple and costless, and it helps attackers better avoid detection.

Hackers Compromised Dropbox eSignature Service

SecurityWeek - 02 May 2024 08:23

Dropbox says hackers breached its Sign production environment and accessed customer email addresses and hashed passwords. The post Hackers Compromised Dropbox eSignature Service appeared first on SecurityWeek.

US and UK Warn of Disruptive Russian OT Attacks

Infosecurity Magazine - 02 May 2024 09:30

The US and its allies claim Russian hacktivists are disruptive operations in water, energy, food and agriculture sectors