Scottish Cyber Coordination Centre

Daily threat bulletin

6 August 2024

Vulnerabilities

Google fixes Android kernel zero-day exploited in targeted attacks

BleepingComputer - 05 August 2024 19:40

Android security updates this month patch 46 vulnerabilities, including a high-severity remote code execution (RCE) exploited in targeted attacks. [...]

Researchers warn of a new critical Apache OFBiz flaw

Security Affairs - 05 August 2024 17:42

Researchers urge organizations using Apache OFBiz to address a critical bug, following reports of active exploitation of another flaw. Experts urge organizations to address a new critical vulnerability, tracked as CVE-2024-38856, in Apache OFBiz.

Researchers Uncover Flaws in Windows Smart App Control and SmartScreen

The Hacker News - 05 August 2024 19:32

Cybersecurity researchers have uncovered design weaknesses in Microsoft's Windows Smart App Control and SmartScreen that could enable threat actors to gain initial access to target environments without raising any warnings.

New SLUBStick Attack Makes Linux Kernel Vulnerabilities More Dangerous

SecurityWeek - 05 August 2024 12:53

A new Linux kernel exploitation technique named SLUBStick makes heap vulnerabilities more dangerous. The post New SLUBStick Attack Makes Linux Kernel Vulnerabilities More Dangerous appeared first on SecurityWeek.

CISA Adds One Known Exploited Vulnerability to Catalog

CISA Advisories -

CISA has added one new vulnerability to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation. CVE-2018-0824 Microsoft COM for Windows Deserialization of Untrusted Data Vulnerability.

Threat actors and malware

Ransomware gang targets IT workers with new SharpRhino malware

BleepingComputer - 05 August 2024 18:09

The Hunters International ransomware group is targeting IT workers with a new C# remote access trojan (RAT) called SharpRhino to breach corporate networks. [...]

North Korean hackers exploit VPN update flaw to install malware

BleepingComputer - 05 August 2024 14:21

South Korea's National Cyber Security Center (NCSC) warns that state-backed DPRK hackers hijacked flaws in a VPN's software update to deploy malware and breach networks. [...]

New LianSpy malware hides by blocking Android security feature

BleepingComputer - 05 August 2024 12:23

A previously undocumented Android malware named 'LightSpy' has been discovered targeting Russian users, posing on phones as an Alipay app or a system service to evade detection. [...]

Russia's 'Fighting Ursa' APT Uses Car Ads to Install HeadLace Malware

darkreading - 05 August 2024 12:38

The scheme, from the group also known as APT28, involves targeting Eastern European diplomats in need of personal transportation and tempting them with a purported good deal on a Audi Q7 Quattro SUV.