



Daily threat bulletin

21 November 2024

Vulnerabilities

[Decades-Old Security Vulnerabilities Found in Ubuntu's Needrestart Package](#)

The Hacker News - 20 November 2024 15:46

Multiple decade-old security vulnerabilities have been disclosed in the needrestart package installed by default in Ubuntu Server (since version 21.04) that could allow a local attacker to gain root privileges without requiring user interaction.

[Apple Urgently Patches Actively Exploited Zero-Days](#)

darkreading - 20 November 2024 16:05

Though information regarding the exploits is limited, the company did report that Intel-based Mac systems have been targeted by cybercriminals looking to exploit CVE-2024-44308 and CVE-2024-44309.

Threat actors and malware

[New Ghost Tap attack abuses NFC mobile payments to steal money](#)

BleepingComputer - 20 November 2024 12:44

Cybercriminals have devised a novel method to cash out from stolen credit card details linked to mobile payment systems such as Apple Pay and Google Pay, dubbed 'Ghost Tap,' which relays NFC card data to money mules worldwide. [...]

[NodeStealer Malware Targets Facebook Ad Accounts, Harvesting Credit Card Data](#)

The Hacker News - 21 November 2024 13:04

Threat hunters are warning about an updated version of the Python-based NodeStealer that's now equipped to extract more information from victims' Facebook Ads Manager accounts and harvest credit card data stored in web browsers."

[China's 'Liminal Panda' APT Attacks Telcos, Steals Phone Data](#)

darkreading - 20 November 2024 21:35

In US Senate testimony, a CrowdStrike exec explained how this advanced persistent threat penetrated telcos in Asia and Africa, gathering SMS messages, unique identifiers, and other metadata along the way.

[Phobos ransomware indictment sheds light on long-running, quietly successful scheme](#)



Scottish
Cyber
Coordination
Centre

The Record from Recorded Future News - 20 November 2024 22:08