Scottish Cyber Coordination Centre

Daily threat bulletin

11 November 2024

Vulnerabilities

Palo Alto Networks warns of potential PAN-OS RCE vulnerability

BleepingComputer - 08 November 2024 13:42

Palo Alto Networks warned customers to restrict access to their next-generation firewalls because of a potential remote code execution vulnerability in the PAN-OS management interface. [...]

Malicious actors are exploiting DocuSign to send fake invoices

Security Magazine - 08 November 2024 09:00

A new report reveals that malicious actors are exploiting APIs in DocuSign to send fake invoices.

AI & LLMs Show Promise in Squashing Software Bugs

darkreading - 08 November 2024 23:16

Large language models (LLMs) can help app security firms find and fix software vulnerabilities. Malicious actors are on to them too, but here's why defenders may retain the edge.

6 Infotainment Bugs Allow Mazdas to Be Hacked With USBs

darkreading - 08 November 2024 23:01

Direct cyberattacks on vehicles are all but unheard of. In theory though, the opportunity is there to cause real damage — data extraction, full system compromise, even gaining access to safety-critical systems.

Advanced Persistent Teenagers, Okta Bug Allowed Logins Without a Correct Password

Security Boulevard - 11 November 2024 06:00

In episode 354, we discuss the emergence of the term 'Advanced Persistent Teenagers' (APT) as a "new" cybersecurity threat. Recorded just before the election, the hosts humorously predict election outcomes while exploring the rise of teenage hackers responsible for major breaches.

HPE Patches Critical Vulnerabilities in Aruba Access Points

SecurityWeek - 08 November 2024 12:44

HPE this week warned of two critical vulnerabilities in Aruba Networking access points that could lead to unauthenticated command injection.

Scottish Cyber Coordination Centre

Threat actors and malware

Hackers now use ZIP file concatenation to evade detection

BleepingComputer - 10 November 2024 11:13

Hackers are targeting Windows machines using the ZIP file concatenation technique to deliver malicious payloads in compressed archives without security solutions detecting them. [...]

Scammers target UK senior citizens with Winter Fuel Payment texts

BleepingComputer - 09 November 2024 17:08

As the winter season kicks in, scammers are not missing the chance to target senior British residents with bogus “winter heating allowance” and “cost of living support” scam texts. [...]

Veeam Backup & Replication exploit reused in new Frag ransomware attack

Security Affairs - 09 November 2024 18:50

A critical flaw, tracked as CVE-2024-40711, in Veeam Backup & Replication (VBR) was also recently exploited to deploy Frag ransomware. In mid-October, Sophos researchers warned that ransomware operators are exploiting the critical vulnerability CVE-2024-40711 in Veeam Backup & Replication to create rogue accounts and deploy malware.

Cybercriminals Use Excel Exploit to Spread Fileless Remcos RAT Malware

The Hacker News - 11 November 2024 12:43

Cybersecurity researchers have discovered a new phishing campaign that spreads a new fileless variant of known commercial malware called Remcos RAT.

Palo Alto Advises Securing PAN-OS Interface Amid Potential RCE Threat Concerns

The Hacker News - 09 November 2024 12:42

Palo Alto Networks on Friday issued an informational advisory urging customers to ensure that access to the PAN-OS management interface is secured because of a potential remote code execution vulnerability.

SpyAgent malware targets crypto wallets by stealing screenshots

Security Intelligence - 08 November 2024 15:00

A new Android malware strain known as SpyAgent is making the rounds — and stealing screenshots as it goes. Using optical character recognition (OCR) technology, the malware is after cryptocurrency recovery phrases often stored in screenshots on user devices. Here’s how to dodge the bullet.