Scottish Cyber Coordination Centre

Daily threat bulletin

15 November 2024

Vulnerabilities

CISA warns of more Palo Alto Networks bugs exploited in attacks

BleepingComputer - 14 November 2024 18:01

CISA warned today that two more critical security vulnerabilities in Palo Alto Networks' Expedition migration tool are now actively exploited in attacks. [...]

Fortinet patches VPN app flaw that could give rogue users, malware a privilege boost

The Register - 14 November 2024 23:22

Plus a bonus hard-coded local API key A now-patched, high-severity bug in Fortinet's FortiClient VPN application potentially allows a low-privilege rogue user or malware on a vulnerable Windows system to gain higher privileges from another user, execute code and possibly take over the box, and delete log files....

Varonis Warns of Bug Discovered in PostgreSQL PL/Perl

darkreading - 14 November 2024 22:53

Several versions of PostgreSQL are impacted, and customers will need to upgrade in order to patch.

Five Eyes infosec agencies list 2024's most exploited software flaws

The Register - 14 November 2024 09:31

Slack patching remains a problem – which is worrying as crooks increasingly target zero-day vulns The cyber security agencies of the UK, US, Canada, Australia, and New Zealand have issued their annual list of the 15 most exploited vulnerabilities, and warned that attacks on zero-day exploits have become more common....

Threat actors and malware

New Glove infostealer malware bypasses Chrome's cookie encryption

BleepingComputer - 14 November 2024 16:47

New Glove Stealer information-stealing malware can bypass Google Chrome's Application-Bound (App-Bound) encryption to steal browser cookies. [...]

New RustyAttr Malware Targets macOS Through Extended Attribute Abuse

The Hacker News - 14 November 2024 16:21

Scottish Cyber Coordination Centre

Threat actors have been found leveraging a new technique that abuses extended attributes for macOS files to smuggle a new malware called RustyAttr.The Singaporean cybersecurity company has attributed the novel activity with moderate confidence to the infamous North Korea-linked Lazarus Group, citing infrastructure and tactical overlaps observed in connection with prior campaigns.

Cybercriminals target victims in Spain, Germany, Ukraine with Strela Stealer malware

The Record from Recorded Future News - 14 November 2024 15:28

Cloud Ransomware Flexes Fresh Scripts Against Web Apps

darkreading - 14 November 2024 18:30

Cloud service providers are getting better at protecting data, pushing adversaries to develop new cloud ransomware scripts to target PHP applications, a new report says.

Crimeware and financial cyberthreats in 2025

Securelist - 14 November 2024 10:00

Kaspersky's GReAT looks back on the 2024 predictions about financial and crimeware threats, and explores potential cybercrime trends for 2025.