Scottish
Cyber
Coordination
Centre

Daily threat bulletin

12 September 2024

Vulnerabilities

Progress Software issues fix for maximum severity vulnerability

Security Magazine - 11 September 2024 13:00

Security leaders discuss the maximum severity vulnerability in Progress Software products.

Air-Gapped Networks Vulnerable to Acoustic Attack via LCD Screens

darkreading - 11 September 2024 14:00

In the "PixHell" attack, sound waves generated by pixels on a screen can transmit information across seemingly impenetrable air gaps.

Intel Warns of 20+ Vulnerabilities, Advises Firmware Updates

SecurityWeek - 11 September 2024 14:52

Intel on Tuesday published advisories covering more than 20 vulnerabilities affecting processors and other products.

Microsoft Fixes Four Actively Exploited Zero-Days

Infosecurity Magazine - 11 September 2024 09:30

September’s Patch Tuesday fix-list features scores of CVEs including four zero-day vulnerabilities

[R1] Nessus Version 10.8.3 Fixes Multiple Vulnerabilities

Tenable Product Security Advisories - 11 September 2024 20:19

[R1] Nessus Version 10.8.3 Fixes Multiple Vulnerabilities

[R1] Nessus Version 10.7.6 Fixes Multiple Vulnerabilities

Tenable Product Security Advisories - 11 September 2024 17:57

[R1] Nessus Version 10.7.6 Fixes Multiple Vulnerabilities

[R1] Nessus Agent Version 10.7.3 Fixes Multiple Vulnerabilities

Tenable Product Security Advisories - 11 September 2024 17:29

[R1] Nessus Agent Version 10.7.3 Fixes Multiple Vulnerabilities

Threat actors and malware

Fake password manager coding test used to hack Python developers

BleepingComputer - 11 September 2024 18:09

Members of the North Korean hacker group Lazarus posing as recruiters are baiting Python developers with coding test project for password management products that include malware. [...]

RansomHub ransomware gang relies on Kaspersky TDSKiller tool to disable EDR

Security Affairs - 11 September 2024 14:15

Researchers observed the RansomHub ransomware group using the TDSSKiller tool to disable endpoint detection and response (EDR) systems. The RansomHub ransomware gang is using the TDSSKiller tool to disable endpoint detection and response (EDR) systems, Malwarebytes ThreatDown Managed Detection and Response (MDR) team observed. TDSSKiller a legitimate tool developed by the cybersecurity firm Kaspersky to [...]

Quad7 Botnet Expands to Target SOHO Routers and VPN Appliances

The Hacker News - 11 September 2024 22:50

The operators of the mysterious Quad7 botnet are actively evolving by compromising several brands of SOHO routers and VPN appliances by leveraging a combination of both known and unknown security flaws.Targets include devices from TP-LINK, Zyxel, Asus, Axentra, D-Link, and NETGEAR, according to a new report by French cybersecurity company Sekoia."

How Law Enforcement's Ransomware Strategies Are Evolving

darkreading - 11 September 2024 15:00

The threat of ransomware hasn't gone away. But law enforcement has struck a blow by adjusting its tactics and taking out some of the biggest adversaries in the ransomware scene.

UK related

Cyber crooks shut down UK, US schools, thousands of kids affected

The Register - 11 September 2024 23:43

No class: Black Suit ransomware gang boasts of 200GB haul from one raid Cybercriminals closed some schools in America and Britain this week, preventing kindergarteners in Washington state from attending their first-ever school day and shutting down all internet-based systems for Biggin Hill-area students in England for the next three weeks....

UK's ICO and NCA Sign Memorandum to Boost Reporting and Resilience

Infosecurity Magazine - 11 September 2024 10:15

The Information Commissioner's Office and National Crime Agency have cemented ties with a memorandum of understanding