Scottish Cyber Coordination Centre

Daily threat bulletin

11 September 2024

Vulnerabilities

Ivanti fixes maximum severity RCE bug in Endpoint Management software

BleepingComputer - 10 September 2024 16:28

Ivanti has fixed a maximum severity vulnerability in its Endpoint Management software (EPM) that can let unauthenticated attackers gain remote code execution on the core server. [...]

Microsoft Patch Tuesday security updates for September 2024 addressed four actively exploited zero-days

Security Affairs - 11 September 2024 08:07

Microsoft Patch Tuesday security updates for September 2024 addressed 79 flaws, including four actively exploited zero-day flaws. Microsoft Patch Tuesday security updates for September 2024 addressed 79 vulnerabilities in Windows and Windows Components; Office and Office Components; Azure; Dynamics Business Central; SQL Server; Windows Hyper-V; Mark of the Web (MOTW); and the Remote Desktop Licensing [...]

New PIXHELL Attack Exploits LCD Screen Noise to Exfiltrate Data from Air-Gapped Computers

The Hacker News - 10 September 2024 16:40

A new side-channel attack dubbed PIXHELL could be abused to target air-gapped computers by breaching the “audio gap” and exfiltrating sensitive information by taking advantage of the noise generated by pixels on an LCD screen.

Adobe Patches Critical, Code Execution Flaws in Multiple Products

SecurityWeek - 10 September 2024 17:34

Patch Tuesday: Adobe releases patches for 28 security vulnerabilities and warned of code execution risks on Windows and macOS platforms.

Critical SonicWall SSLVPN Bug Exploited By Ransomware Actors

Infosecurity Magazine - 10 September 2024 09:40

Researchers have warned that a critical SonicWall vulnerability is being exploited in ransomware attacks.

Threat actors and malware

RansomHub ransomware abuses Kaspersky TDSSKiller to disable EDR software

Scottish Cyber Coordination Centre

BleepingComputer - 10 September 2024 15:29

The RansomHub ransomware gang has been using TDSSKiller, a legitimate tool from Kaspersky, to disable endpoint detection and response (EDR) services on target systems. [...]

Quad7 botnet evolves to more stealthy tactics to evade detection

Security Affairs - 10 September 2024 21:08

The Quad7 botnet evolves and targets new SOHO devices, including Axentra media servers, Ruckus wireless routers and Zyxel VPN appliances. The Sekoia TDR team identified additional implants associated with the Quad7 botnet operation.

CosmicBeetle Deploys Custom ScRansom Ransomware, Partnering with RansomHub

The Hacker News - 10 September 2024 22:18

The threat actor known as CosmicBeetle has debuted a new custom ransomware strain called ScRansom in attacks targeting small- and medium-sized businesses (SMBs) in Europe, Asia, Africa, and South America, while also likely working as an affiliate for RansomHub.

Mustang Panda Feeds Worm-Driven USB Attack Strategy

darkreading - 10 September 2024 16:27

A fresh wave of attacks on APAC government entities involves both self-propagating malware spreading via removable drives and a spear-phishing campaign.