Scottish Cyber Coordination Centre

Daily threat bulletin

20 September 2024

Vulnerabilities

Ivanti warns of another critical CSA flaw exploited in attacks

BleepingComputer - 19 September 2024 15:39

Today, Ivanti warned that threat actors are exploiting another Cloud Services Appliance (CSA) security flaw in attacks targeting a limited number of customers. [...]

U.S. CISA adds Microsoft Windows, Apache HugeGraph-Server, Oracle JDeveloper, Oracle WebLogic Server, and Microsoft SQL Server bugs to its Known Exploited Vulnerabilities catalog

Security Affairs - 19 September 2024 16:47

U.S. Cybersecurity and Infrastructure Security Agency (CISA) adds Microsoft Windows, Apache HugeGraph-Server, Oracle JDeveloper, Oracle WebLogic Server, and Microsoft SQL Server bugs to its Known Exploited Vulnerabilities catalog. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added SonicWall SonicOS, ImageMagick and Linux Kernel vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog.

1 PoC Exploit for Critical RCE Flaw, but 2 Patches From Veeam

darkreading - 19 September 2024 20:57

The first patch lets threat actors with low-level credentials still exploit the vulnerability, while the second fully resolves the flaw.

CISA: Oracle Vulnerabilities From 'Miracle Exploit' Targeted in Attacks

SecurityWeek - 19 September 2024 14:05

CISA is warning organizations that two Oracle vulnerabilities tracked as CVE-2022-21445 and CVE-2020-14644 are being exploited in the wild.

Atlassian Patches Vulnerabilities in Bamboo, Bitbucket, Confluence, Crowd

SecurityWeek - 19 September 2024 12:53

Atlassian's September 2024 monthly security bulletin details multiple high-severity vulnerabilities in four products.

Threat actors and malware

North Korean APT Bypasses DMARC Email Policies in Cyber-Espionage Attacks

darkreading - 20 September 2024 02:00

How the Kimsuky nation-state group and other threat actors are exploiting poor email security — and what organizations can do to defend themselves.

FBI Leads Takedown of Chinese Botnet Impacting 200K Devices

darkreading - 19 September 2024 15:55

Once a user's device is infected as part of an ongoing Flax Typhoon APT campaign, the malware connects it to a botnet called Raptor Train, initiating malicious activity.

Infostealers Cause Surge in Ransomware Attacks, Just One in Three Recover Data

Infosecurity Magazine - 19 September 2024 17:15

Infostealer malware and digital identity exposure behind rise in ransomware, researchers find.

UK related

Malicious actors target UK motorists with QR code scams

Security Magazine - 19 September 2024 09:00

Motorists in the United Kingdom are being targeted with QR code scams.

UK activists targeted with Pegasus spyware ask police to charge NSO Group

The Register - 19 September 2024 13:16

4 file complaint with London's Met, alleging malware maker helped autocratic states violate their privacy Four UK-based proponents of human rights and critics of Middle Eastern states today filed a report with London's Metropolitan Police they hope will lead to charges against Pegasus peddler NSO Group.