Scottish Cyber Coordination Centre

Daily Threat Bulletin

20 August 2024

Vulnerabilities

CISA warns of Jenkins RCE bug exploited in ransomware attacks

BleepingComputer - 19 August 2024 16:16

CISA has added a critical Jenkins vulnerability that can be exploited to gain remote code execution to its catalog of security bugs, warning that it's actively exploited in attacks.

Experts warn of exploit attempt for Ivanti vTM bug

Security Affairs - 19 August 2024 10:35

Researchers at the Shadowserver Foundation observed an exploit attempt based on the public proof of concept (PoC) for the Ivanti vTM bug, CVE-2024-7593.

Microsoft Patches Zero-Day Flaw Exploited by North Korea’s Lazarus Group

The Hacker News - 19 August 2024 13:35

A newly patched security flaw in Microsoft Windows was exploited as a zero-day by Lazarus Group, a prolific state-sponsored actor affiliated with North Korea. The security vulnerability, tracked as CVE-2024-38193 (CVSS score: 7.8), has been described as a privilege escalation bug in the Windows Ancillary Function Driver (AFD.sys) for WinSock.

Microsoft Apps for macOS Exposed to Library Injection Attacks

Infosecurity Magazine - 19 August 2024 15:15

Cisco Talos researchers found a flaw in eight Microsoft apps for macOS that could enable library injection attacks, putting sensitive data at risk

Threat actors and malware

New UULoader Malware Distributes Gh0st RAT and Mimikatz in East Asia

The Hacker News - 19 August 2024 19:36

A new type of malware called UULoader is being used by threat actors to deliver next-stage payloads like Gh0st RAT and Mimikatz. The Cyberint Research Team, which discovered the malware, said it's distributed in the form of malicious installers for legitimate applications targeting Korean and Chinese speakers.

Cybercriminals Exploit Popular Software Searches to Spread FakeBat Malware

The Hacker News - 19 August 2024 19:07

Cybersecurity researchers have uncovered a surge in malware infections stemming from malvertising campaigns distributing a loader called FakeBat. "These attacks are opportunistic in nature, targeting users seeking popular business software," the Mandiant Managed Defense team said in a technical report.

New Tool Xeon Sender Enables Large-Scale SMS Spam Attacks

Infosecurity Magazine - 19 August 2024 16:30

Xeon Sender features SMS spam via APIs, Nexmo/Twilio credentials validation and phone number generation