Scottish Cyber Coordination Centre

Daily threat bulletin

29 May 2024

Vulnerabilities

Exploit released for maximum severity Fortinet RCE bug, patch now

BleepingComputer - 28 May 2024 13:16

Security researchers have released a proof-of-concept (PoC) exploit for a maximum-severity vulnerability in Fortinet's security information and event management (SIEM) solution, which was patched in February.

Courtroom Recording Software Vulnerable to Backdoor Attacks

Infosecurity Magazine - 28 May 2024 12:40

Rapid7 warned that users of Justice AV Solutions (JAVS) Viewer v8.3.7 recording software are at high risk of stolen credentials and having malware installed.

CISA Adds One Known Exploited Vulnerability to Catalog

CISA Advisories -

CISA has added one new vulnerability to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation.CVE-2024-5274 Google Chromium V8 Type Confusion Vulnerability.

Threat actors and malware

Microsoft links North Korean hackers to new FakePenny ransomware

BleepingComputer - 28 May 2024 14:58

Microsoft has linked a North Korean hacking group it tracks as Moonstone Sleet to FakePenny ransomware attacks, which have led to millions of dollars in ransom demands.

Researchers Warn of CatDDoS Botnet and DNSBomb DDoS Attack Technique

The Hacker News - 28 May 2024 16:45

The threat actors behind the CatDDoS malware botnet have exploited over 80 known security flaws in various software over the past three months to infiltrate vulnerable devices and co-opt them into a botnet for conducting distributed denial-of-service (DDoS) attacks

Attackers Target Check Point VPNs to Access Corporate Networks

darkreading - 28 May 2024 20:25

Using VPNs as an initial access vector is ironic, given that security is the very reason enterprises employ them in the first place.

Scottish
Cyber
Coordination
Centre