Scottish Cyber Coordination Centre

Daily threat bulletin

18 June 2024

Vulnerabilities

From Risk to Resolution: OX Security's Integrations with KEV and EPSS Drive Smarter Vulnerability Prioritization

Security Boulevard - 17 June 2024 20:54

In June 2023, a critical vulnerability (CVE-2023-34362) in the MOVEit Transfer file transfer software was exploited by adversaries, resulting in a series of high-profile data breaches. Despite the availability of patches, and the vulnerability being publicly known and actively exploited, many organizations failed to prioritize its remediation.

VMware by Broadcom warns of two critical vCenter flaws, plus a nasty sudo bug

The Register - 18 June 2024 07:08

Specially crafted network packet could allow remote code execution and access to VM fleets VMware by Broadcom has revealed a pair of critical-rated flaws in vCenter Server – the tool used to manage virtual machines and hosts in its flagship Cloud Foundation and vSphere suites.

Threat actors and malware

Hackers use F5 BIG-IP malware to stealthily steal data for years

BleepingComputer - 17 June 2024 14:37

A group of suspected Chinese cyberespionage actors named 'Velvet Ant' are deploying custom malware on F5 BIG-IP appliances to gain a persistent connection to the internal network and steal data.

Hackers Exploit Legitimate Websites to Deliver BadSpace Windows Backdoor

The Hacker News - 17 June 2024 12:58

Legitimate-but-compromised websites are being used as a conduit to deliver a Windows backdoor dubbed BadSpace under the guise of fake browser updates."The threat actor employs a multi-stage attack chain involving an infected website, a command-and-control (C2) server, in some cases a fake browser update, and a JScript downloader to deploy a backdoor into the victim's system.

Only 19% of MITRE ATT&CK tactics are covered by SIEMs

Security Magazine - 17 June 2024 09:00

Security leaders respond to a new report showing only 19% of MITRE ATT&CK tactics are covered by SIEMs.

Scottish Cyber Coordination Centre

Notorious cyber gang UNC3944 attacks vSphere and Azure to run VMs inside victims' infrastructure

The Register - 17 June 2024 07:34

Who needs ransomware when you can scare techies into coughing up their credentials? Notorious cyber gang UNC3944 – the crew suspected of involvement in the recent attacks on Snowflake and MGM Entertainment, and plenty more besides – has changed its tactics and is now targeting SaaS applications.