Scottish Cyber Coordination Centre

Daily threat bulletin

8 January 2025

Vulnerabilities

CISA Flags Critical Flaws in Mitel and Oracle Systems Amid Active Exploitation

The Hacker News - 08 January 2025 10:51

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Tuesday added three flaws impacting Mitel MiCollab and Oracle WebLogic Server to its Known Exploited Vulnerabilities (KEV) catalog, citing evidence of active exploitation.The list of vulnerabilities is as follows -CVE-2024-41713 (CVSS score: 9.1) - A path traversal vulnerability in Mitel MiCollab that could allow an attacker

Researchers Uncover Major Security Flaw in Illumina iSeq 100 DNA Sequencers

The Hacker News - 07 January 2025 20:52

Cybersecurity researchers have uncovered firmware security vulnerabilities in the Illumina iSeq 100 DNA sequencing instrument that, if successfully exploited, could permit attackers to brick or plant persistent malware on susceptible devices.

New Research Highlights Vulnerabilities in MLOps Platforms

Infosecurity Magazine - 07 January 2025 18:15

New research by Security Intelligence has revealed security risks in MLOps platforms including Azure ML, BigML and Google Vertex AI

Moxa Urges Immediate Updates for Security Vulnerabilities

Infosecurity Magazine - 07 January 2025 17:30

Moxa has reported two critical vulnerabilities in its routers and network security appliances that could allow system compromise and arbitrary code execution

Dell, HPE, MediaTek Patch Vulnerabilities in Their Products

SecurityWeek - 07 January 2025 14:05

MediaTek, HPE and Dell release advisories to inform customers about potentially serious vulnerabilities found and patched in their products.

Threat actors and malware

New Mirai botnet targets industrial routers with zero-day exploits

BleepingComputer - 07 January 2025 16:44

A relatively new Mirai-based botnet has been growing in sophistication and is now leveraging zero-day exploits for security flaws in industrial routers and smart home devices. [...]

Malicious Browser Extensions are the Next Frontier for Identity Attacks

BleepingComputer - 07 January 2025 11:02

A recent campaign targeting browser extensions illustrates that they are the next frontier in identity attacks. Learn more about these attacks from LayerX Security and how to receive a free extension audit. [...]

New EAGERBEE Variant Targets ISPs and Governments with Advanced Backdoor Capabilities

The Hacker News - 07 January 2025 16:16

Internet service providers (ISPs) and governmental entities in the Middle East have been targeted using an updated variant of the EAGERBEE malware framework.The new variant of EAGERBEE (aka Thumtais) comes fitted with various components that allow the backdoor to deploy additional payloads, enumerate file systems, and execute commands shells, demonstrating a significant evolution.