Scottish Cyber Coordination Centre

Daily Threat Bulletin

21 February 2025

Vulnerabilities

Atlassian Patches Critical Vulnerabilities in Confluence, Crowd

SecurityWeek - 20 February 2025 14:34

Atlassian has released patches for 12 critical- and high-severity vulnerabilities in Bamboo, Bitbucket, Confluence, Crowd, and Jira.

PoC Exploit Published for Critical Ivanti EPM Vulnerabilities

SecurityWeek - 20 February 2025 12:41

Proof-of-concept (PoC) code and technical details on four critical-severity Ivanti EPM vulnerabilities are now available.

Microsoft testing fix for Windows 11 bug breaking SSH connections

BleepingComputer - 20 February 2025 09:19

Microsoft is now testing a fix for a longstanding known issue that is breaking SSH connections on some Windows 11 22H2 and 23H2 systems.

Critical flaws in Mongoose library expose MongoDB to data thieves, code execution

The Register - 20 February 2025 15:45

Bugs fixed, updating to the latest version is advisable Security sleuths found two critical vulnerabilities in a third-party library that MongoDB relies on, which means adversaries can potentially steal data and run code.

Threat actors and malware

Chinese hackers use custom malware to spy on US telecom networks

BleepingComputer - 20 February 2025 12:11

The Chinese state-sponsored Salt Typhoon hacking group uses a custom utility called JumbledPath to stealthily monitor network traffic and potentially capture sensitive data in cyberattacks on U.S. telecommunication providers.

NailaoLocker ransomware targets EU healthcare-related entities

Security Affairs - 20 February 2025 16:47

Orange Cyberdefense CERT uncovered a malware campaign, tracked as The Green Nailao campaign, that targeted European organizations, including healthcare, in late 2024, using ShadowPad, PlugX, and the previously undocumented NailaoLocker ransomware.

Scottish Cyber Coordination Centre

Cybercriminals Use Eclipse Jarsigner to Deploy XLoader Malware via ZIP Archives

The Hacker News - 20 February 2025 17:42

A malware campaign distributing the XLoader malware has been observed using the DLL side-loading technique by making use of a legitimate application associated with the Eclipse Foundation.

'Darcula' Phishing Kit Can Now Impersonate Any Brand

darkreading - 20 February 2025 12:00

With Version 3, would-be phishers can cut and paste a big brand's URL into a template and let automation do the rest.

Google Docs used by infostealer ACRStealer as part of attack

Malwarebytes - 20 February 2025 16:49

An infostealer known as ACRStealer is using legitimate platforms like Google Docs and Steam as part of an attack.