Daily Intelligence Update | 14 October 2025

China's National Computer Network Emergency Response Technical Team and Coordination Center (CNCERT/CC) has accused U.S. intelligence agencies of escalating cyber operations against its defense and military sectors. According to the statement, these attacks have become increasingly covert and targeted, with the goal of stealing sensitive military research, design plans, and core production information. CNCERT/CC highlighted two incidents: between July 2022 and July 2023, U.S. agencies allegedly exploited a Microsoft Exchange zero-day to control a Chinese military enterprise's email servers for nearly a year, exfiltrating communications from 11 individuals across more than 40 separate attacks. The intrusions reportedly leveraged multiple foreign IP addresses and sophisticated obfuscation techniques to avoid detection. A second campaign between July and November 2024 allegedly targeted the electronic file system of a Chinese communications contractor, allowing malware implants to control over 300 devices. Investigators claim the attackers focused on terms such as "military network" and "core network," pointing to deliberate and strategic targeting.

Separately, researchers released additional findings on a critical extortion campaign tied to exploitation of Oracle E-Business Suite (EBS). The activity centers on CVE-2025-61882, an unauthenticated remote code execution vulnerability that Oracle patched on October 4. Evidence shows exploitation began as early as July 10, 2025, with attackers chaining multiple zero-day flaws against UiServlet and SyncServlet components to deliver in-memory Java payloads such as GOLDVEIN and the SAGEGIFT/SAGELEAF/SAGEWAVE variants. Infrastructure analysis revealed activity from IPs including 200.107.207[.]26, along with the circulation of a leaked exploit archive in Telegram channels linked to Scattered LAPSUS$ Hunters. Following initial access and data theft, operators launched an extortion campaign on September 29, contacting executives from compromised third-party accounts while leveraging the Cl0p brand to pressure for payment. While Oracle initially speculated previously patched flaws might have been reused, researchers confirmed the attacks exploited CVE-2025-61882 as a zero-day. Overlaps in tooling, infrastructure, and tactics point to Cl0p, FIN11, or associated clusters. Oracle has urged immediate patching, outbound traffic restrictions, memory forensics, and database artifact searches to detect active compromise.

In parallel, CISA has added CVE-2025-32463, a critical vulnerability in the Sudo utility, to its Known Exploited Vulnerabilities (KEV) catalog. The flaw, affecting all Sudo versions prior to 1.9.17p1, allows local attackers to escalate privileges and execute arbitrary commands as root by abusing the --chroot (-R) option, even if they are not listed in the sudoers file. First reported in July 2025, the vulnerability is now confirmed to be under active exploitation in the wild, though attribution remains unclear. CISA advises organizations to upgrade immediately to patched versions to mitigate privilege escalation risks.
