US Air Force Cloud One platform reportedly breached amid wave of federal incidents



Hackers reportedly breached the US Air Force's Cloud One platform via an unidentified vulnerability, joining recent incidents at US agencies. The FBI also warned about ARTEX, an AI-driven attack framework.

- Reuters reports the intrusion was found within the past month during a platform upgrade, disrupting migrations and software updates.
- A source says attackers used an unidentified software vulnerability; the attackers, scope and any data theft remain unknown.
- Recent incidents also reportedly hit the FBI's NCIC, a CIA OSINT system and FinCEN; links between them are unclear.
- The FBI says ARTEX, an open-source AI penetration framework, has been used since at least August

2026, with some intrusions reaching privileged access in under three hours.

- Whether ARTEX was used against the Air Force, FBI or FinCEN is not known.

Hackers have reportedly breached Cloud One, the US Air Force's enterprise cloud platform, according to Reuters as cited by BleepingComputer. The platform, launched in 2017, lets Department of Defense agencies host applications for operations, personnel, logistics and maintenance.

What is known

The intrusion was reportedly discovered within the past month during a platform upgrade, which disrupted application migrations and software updates. One source said attackers exploited an unidentified software vulnerability, potentially exposing sensitive operational and logistics information. US Cyber Command has reportedly been called in. The attackers, the scope and whether data was stolen are unknown. The Air Force declined to comment on the status of the systems.

The report follows other disclosed incidents: the FBI's National Crime Information Center, a CIA open-source intelligence analysis system (also affecting ODNI and NGA), and an investigation by FinCEN into unauthorized access. It is unclear whether these are connected.

AI-driven attack tooling

The CIA breach was reportedly conducted with ARTEX, which the FBI says multiple actors have used since at least August 2026 against government, defense, healthcare, financial and technology targets. The framework automates vulnerability discovery, privilege escalation and data theft, and connects to external AI models. Some intrusions reached privileged access in under three hours. Researchers found more than 1,600 exposed ARTEX management consoles by early November.

The source does not say whether ARTEX was used against the Air Force, FBI or FinCEN. Saudi institutions should treat this as a prompt to review cloud platform change windows, patch speed and detection, rather than as a confirmed threat to their own environments.

What to do now

1. Review security controls around planned cloud platform upgrades and migrations, including monitoring during change windows.
2. Check that patching of internet-facing and cloud-hosted software is prioritized and measured against fast attacker timelines.
3. Test whether detection and response can contain privilege escalation within hours, not days.
4. Review privileged access to cloud platforms and enforce strong authentication and logging.
5. Brief the board and incident response team on AI-automated attacks and confirm escalation paths to the

relevant national authorities.