European Commission confirms AI-assisted cyberattack that disrupted services



The European Commission says an AI-assisted attack detected on 22 October disrupted several services. It is largely contained, with no evidence so far of a staff data breach, and the investigation continues.

- The attack was detected on 22 October and confirmed on 26 October; the Commission says it is largely contained.
- Several applications were taken down as a precaution, and most have been restored.
- Politico reports disruption lasting over 10 days, affecting Sysper, MyPMO and translation systems.
- The Commission confirmed an AI tool was used but named neither the tool nor a known group, and is unaware of any ransom demand.
- CERT-EU had earlier warned about threat actors using the AI penetration-testing framework Artex

> and expects faster, more scalable automated attacks.

The European Commission has confirmed it was hit by a cyberattack in which the attackers used an AI tool. According to spokesperson Thomas Regnier, the attack was detected on 22 October and confirmed on 26 October. It has been largely contained, and the investigation is still under way.

What happened

As a protective measure, the Commission temporarily took several applications offline, and most have since been restored. Regnier said the investigation has found no evidence of a data breach affecting Commission staff. Politico, however, reports that the attackers may have compromised large amounts of data and that disruption lasted more than 10 days, affecting the HR platform Sysper, the medical reimbursement system MyPMO and translation systems.

The Commission did not name the AI tool, did not attribute the attack to a known group, and said it was not aware of a ransom demand.

Wider context

The disclosure came about two weeks after CERT-EU warned that threat actors were using Artex, an AI-powered penetration-testing framework, against its constituency. CERT-EU assessed that Artex's public availability will likely speed up adoption by attackers, leading to more frequent, faster and more scalable automated attacks with a higher success rate. The source adds that Artex has been used against organizations including Barracuda, Railway and ConnectWise customers.

Why it matters

The source does not link the Commission incident to Artex. Still, it shows that AI-assisted intrusion is now a documented reality against a major public institution, and that containment can mean taking business-critical applications offline for days. Regulated institutions should treat this as a prompt to review detection speed, isolation options and recovery priorities rather than as a cause for alarm.

What to do now

1. Review detection and alerting thresholds so that fast, automated intrusion activity is flagged and escalated within hours, not days.
2. Pre-agree which business applications can be isolated or taken offline during an incident, with owners and approval paths documented.
3. Test recovery of HR, benefits and other internal platforms, and confirm restoration priorities in your BCM plans.
4. Assess exposure to AI-driven penetration-testing tools by running regular external attack-surface checks

and patching internet-facing systems promptly.

5. Update incident response playbooks to cover AI-assisted attacks, including how to assess data exposure when evidence is still incomplete.