AFP takes its Forum content platform offline after cyberattack



AFP confirmed a cyberattack on AFP Forum, the platform clients use to download its stories, photos and videos. The platform was taken offline as a precaution and remained unavailable on Friday; the scope and the attacker are unknown.

- AFP Forum, used by news outlets to browse and download AFP stories, photos and videos, was targeted overnight.
- AFP detected the intrusion, moved to contain it and took the platform offline as a precaution.
- External cybersecurity experts are assisting the investigation.
- No attacker has been named, no restoration timeline given, and it is unclear whether data was accessed or other systems were affected.
- AFP reported an earlier attack in September 2024 that disrupted some content delivery services.

French news agency Agence France-Presse (AFP) was hit by a cyberattack overnight, according to an internal email to staff that the agency quoted in its own reporting. The target was AFP Forum, an online platform where news outlets browse and download AFP stories, photographs and videos.

What is known

AFP says its teams contained the intrusion as soon as it was detected and took AFP Forum offline as a precaution. The platform stayed unavailable on Friday, showing a maintenance notice in several languages. According to French media reports, subscribers are being offered alternative ways to reach the content in the meantime. The agency is investigating with external cybersecurity experts.

What is not known

AFP has not said who was behind the attack or when the service will return. It is unclear whether sensitive information was accessed or whether other AFP systems were affected. The agency did not respond to a request for comment. This is not the first such incident: in September 2024 AFP detected an attack on its IT systems that disrupted some services used to deliver content to subscribers, and that attack has not been publicly attributed.

Why it matters

The case shows how an external-facing platform that clients depend on can become a single point of disruption, and how a precautionary shutdown is a legitimate containment choice with real service consequences. Institutions that publish data or content to customers through portals can use it as a prompt to test their own containment and fallback arrangements.

What to do now

1. Inventory customer-facing portals and download platforms and confirm each has a named owner and an incident contact.
2. Pre-approve criteria and authority for taking an external platform offline as a containment step.
3. Prepare and test fallback channels so customers can still receive essential content or data during an outage.
4. Check that logging on public-facing platforms is sufficient to determine later whether data was accessed.
5. Review notification duties to the relevant regulator and affected customers if an intrusion is confirmed, and rehearse them in a tabletop exercise.