Microsoft Agent Framework PyPI package trojanized to steal cloud credentials



Researchers report that Microsoft's agent-framework Python package was compromised. Versions 1.26.1 and 1.26.2, published on 17 November 2026, run a credential stealer whenever Python starts.

- Malicious versions 1.26.1 and 1.26.2 of Microsoft's agent-framework package were published to PyPI 33 minutes apart on 17 November 2026.
- The code is built to run a credential stealer each time Python starts.
- The incident is reported by several security firms, including Aikido, Chainguard, Endor Labs, OX Security, SafeDep, Socket, StepSecurity and Wiz.
- The stated aim is theft of cloud credentials.

What happened

Several security vendors report that Microsoft's agent-framework package on PyPI was compromised and used to distribute a credential stealer. Two malicious releases, 1.26.1 and 1.26.2, were published 33 minutes apart on 17 November 2026.

Why it matters

According to the reports, the malicious versions are designed to run the stealer every time Python starts. This means that simply having an affected version installed in an environment may be enough to trigger execution, without anyone calling the package directly. The reported objective is theft of cloud credentials, which could give an attacker access to cloud accounts and the data and workloads behind them.

The source excerpt does not say how the publishing access was obtained, how long the versions stayed available, or how many environments were affected. Institutions should avoid assuming either exposure or safety until they check their own estates.

What to do next

Treat this as a software supply chain incident. Establish whether versions 1.26.1 or 1.26.2 were installed anywhere, including developer machines, build pipelines, containers and cloud notebooks. Where they were, assume any credentials reachable from that environment may be exposed and rotate them. Follow the guidance published by the vendors named above and by Microsoft as it develops.

What to do now

1. Search all Python environments, build pipelines, containers and lock files for agent-framework versions 1.26.1 and 1.26.2.
2. Where either version was installed, rotate cloud credentials, tokens and secrets reachable from that environment.
3. Review cloud audit logs for unusual sign-ins or API activity from the affected identities.
4. Pin dependency versions and use an internal package mirror or approval step for new releases.
5. Record the incident under your third-party and supply chain risk process and notify your security operations team.