

SAP patches maximum-severity OAuth2 credential theft flaw in Cloud SDK for Python



SAP has patched CVE-2026-89111, a maximum-severity OAuth2 SSRF vulnerability in its Cloud SDK for Python that allows remote attackers to steal credentials from multi-tenant BTP applications.

- CVE-2026-89111 is a maximum-severity OAuth2 SSRF flaw in SAP Cloud SDK for Python affecting multi-tenant BTP applications
- Remote attackers can exploit the vulnerability without privileges by controlling the tenant_subdomain parameter to redirect OAuth2 token requests and steal client credentials
- SAP released October 2026 security updates addressing 20 vulnerabilities across multiple products, including two additional critical flaws
- Temporary mitigation available through allowlist validation of tenant_subdomain values for

organizations unable to patch immediately

- CISA has catalogued 14 SAP vulnerabilities as actively exploited since November 2021, three used in ransomware campaigns

Vulnerability details

SAP has released its October 2026 security updates addressing 20 vulnerabilities across its product portfolio, headlined by CVE-2026-89111, a maximum-severity flaw in the Cloud SDK for Python. The SDK serves as the official programmatic toolkit for developing AI agents and Python applications on SAP Business Technology Platform services.

The **OAuth2 SSRF vulnerability** affects multi-tenant BTP applications and can be exploited by remote attackers without requiring any privileges. By controlling the `tenant_subdomain` parameter, attackers can redirect OAuth2 token requests to attacker-controlled servers, causing client credentials to be exfiltrated. SAP has confirmed that organizations unable to deploy patches immediately can temporarily mitigate the risk by validating `tenant_subdomain` values against a known allowlist of registered tenant subdomains before passing them to SDK calls.

Additional critical flaws patched

The October update also addresses CVE-2026-89110, a critical broken access control vulnerability in SAP NetWeaver Visual Composer that permits remote attackers with limited privileges to fully compromise vulnerable systems. A third critical flaw, CVE-2026-89108, affects SAP Manufacturing Integration and Intelligence, allowing threat actors with administrator privileges to provision elevated-privilege accounts on the underlying Java application and gain admin control over the system.

Broader context

SAP has patched several maximum-severity vulnerabilities in recent months, including CVE-2026-58231 in Commerce Cloud in August, which was flagged as actively exploited shortly after disclosure. The U.S. Cybersecurity and Infrastructure Security Agency has catalogued 14 SAP security flaws as actively exploited since November 2021, with three confirmed as leveraged in ransomware attacks. SAP serves 99 of the world's 100 largest companies and reported revenues exceeding €36 billion in fiscal year 2025.

What to do now

1. Identify all SAP Cloud SDK for Python deployments and multi-tenant BTP applications within your environment immediately
2. Apply SAP's October 2026 security patches for CVE-2026-89111, CVE-2026-89110, and CVE-2026-89108 as a priority
3. If immediate patching is not feasible, implement allowlist validation for `tenant_subdomain` values before

passing them to SDK calls

4. Review access controls and privilege assignments for SAP NetWeaver Visual Composer and SAP Manufacturing Integration and Intelligence systems
5. Monitor OAuth2 token request patterns and credential usage for anomalies that may indicate exploitation attempts
6. Coordinate with your SAP support team to verify patch deployment and confirm mitigation effectiveness across all affected systems