SAP confirms security incident tied to suspicious GitHub activity



SAP says it detected suspicious activity and acted to protect customers, with no evidence so far of unauthorized access to customer business data. Press reports describe stolen employee tokens and altered source code on GitHub.

- SAP confirmed it identified suspicious activity in its IT environment and took protective measures.
- The company reports no evidence so far of unauthorized access to customer business data.
- Der Spiegel, citing an internal memo, reported an attack tracked as "Project Granite"; attackers reportedly stole employee authentication tokens and copied and modified source code on GitHub.
- SAP did not say which environments were affected or whether customers consuming code from its GitHub repositories need to act.
- Germany's BSI separately warned about agentic AI tools that facilitate cyberattacks.

SAP has confirmed to BleepingComputer that it identified suspicious activity in its IT environment and moved quickly to protect customers. The company states that its investigation so far has found no evidence of unauthorized access to customer business data.

What has been reported

Der Spiegel, citing an internal SAP memo, reported that the company is handling an attack under the code name "Project Granite". According to the outlet's sources, attackers breached SAP's GitHub environment, possibly with the help of AI tools. They reportedly stole authentication tokens belonging to employees and used them to copy and modify source code. SAP has not confirmed these technical details.

What remains unclear

SAP has not said which environments were affected. It also has not said whether customers who download code from its GitHub repositories, or who receive updates fetched directly or indirectly from them, should take any action. A spokesperson declined to provide further information.

Separately, Germany's BSI recently warned about agentic AI tools that empower cyberattacks and urged organizations to focus on incident response and recommended hardening practices.

Practical view

For institutions that run SAP, there is no confirmed customer impact at this stage. The sensible course is to stay calm, confirm what SAP components and repositories your teams rely on, and watch for vendor communication as the investigation develops.

What to do now

1. Inventory which SAP products, add-ons and GitHub-hosted SAP code or packages your teams use or pull updates from.
2. Ask your SAP account contact for written guidance on whether any repositories or update channels are affected.
3. Verify the integrity and provenance of any SAP-sourced code or packages pulled from GitHub recently before deploying them.
4. Review your own GitHub and developer accounts: rotate long-lived tokens, enforce MFA and apply least-privilege access.
5. Record the event in your third-party risk register and brief the CISO, in line with NCA ECC third-party and SAMA CSF requirements.
6. Confirm incident response playbooks cover supplier-originated incidents and token theft.