SAP confirms cyber incident as reports point to source code exposure



SAP has confirmed a cybersecurity incident after reports that attackers entered its GitHub-hosted development environment. The company says it has found no evidence that customer business data was accessed.

- SAP confirmed suspicious activity and said it acted to protect customers and secure its services.
- Der Spiegel reported that attackers used stolen employee authentication tokens in SAP's GitHub environment to copy and modify source code.
- SAP reportedly restricted GitHub access, paused automated development processes and replaced keys used to verify software authenticity.
- It is unclear whether proprietary code was accessed or whether altered code reached customers.
- A separate April attack planted malicious code in several SAP open-source packages; a link between

> the two is unknown.

SAP, the German enterprise software vendor, has confirmed a cybersecurity incident following press reports that attackers breached its software development infrastructure and may have reached its source code.

What has been reported

In a statement, SAP said it identified suspicious activity and moved to protect customers and secure its services. It said its investigation so far has found no evidence of unauthorized access to customer business data. It did not describe the nature or scope of the intrusion.

Der Spiegel reported that the attackers targeted SAP's development environment on GitHub and obtained employee authentication tokens, allowing them to copy and modify code. Handelsblatt reported an internal response effort named "Project Granite". Emergency measures reportedly affected several development teams: GitHub access was restricted, automated development processes were halted, and keys used to confirm that software is genuine were replaced.

What is not known

It is unclear whether proprietary source code was accessed, or whether any modified code ended up in software delivered to customers. SAP has not named the attackers, explained how they got in, or said whether the incident is fully contained.

The incident follows an April supply chain attack in which malicious code was inserted into several open-source packages developed by SAP, aimed at stealing sensitive information from developers and automated build environments. Whether the two events are connected is not known.

Why it matters

SAP products support accounting, procurement, supply chains and human resources at businesses and public institutions worldwide. Organizations that run SAP should treat this as a supplier risk event: the facts are still emerging, and the company's own statement points to no customer data exposure so far.

What to do now

1. Ask your SAP account team for written updates on the incident, including whether delivered software or updates were affected.
2. Watch SAP security notices and verify the authenticity of any patches or packages before deploying them.
3. Review SAP open-source packages used in your developer and build environments in light of the April attack.
4. Rotate tokens and credentials used for GitHub and CI/CD pipelines in your own organization, and enforce

least privilege.

5. Record the event in your third-party risk register and confirm incident notification terms in your SAP contracts.