saas-attacks/techniques/webhooks/description.md at main · pushsecurity/saas-attacks

By jukelennings

Archived: 2026-04-06 01:12:13 UTC

Latest commit

Aug 17, 2023

ID: SAT1039

Tactics

- Defense Evasion
- Exfiltration

Summary

Some SaaS apps allow webhooks to be configured so callbacks are made when certain events are triggered. For example, a webmail platform may allow a webhook callback when a new email is received.

This is useful to an adversary looking to extract new data as it is created from that API. This could be new emails, new files, a real-time view into channels in instant messaging apps, etc.

Adversaries using this technique may also evade detection controls as these are not requests made to the SaaS app (showing in logs) but rather requests to an attacker app made from the app.

Examples

- Microsoft 365

References

- MITRE ATT&CK - Exfiltration Over Web Service
