What is JWT signing key theft?

JWT signing key theft is stealing the private key that an identity provider uses to sign JSON Web Tokens, for example an EdDSA key. With it, an attacker mints valid tokens for any user or service on demand, and because the tokens are cryptographically valid and short-lived, they pass verification and evade static-credential detection. Defend by storing signing keys in an HSM, rotating them, and monitoring token issuance.

HOW IT WORKS

01 How it works and example

The attacker exfiltrates the private signing key, for instance an EdDSA key, from a compromised host, secret store, or memory. They then mint valid, short-lived identity tokens for any principal on demand, impersonating users or services at will. Because each forged token is cryptographically valid and expires quickly, detection tuned for leaked static credentials does not catch it, as seen in a 2026 intrusion.

SOURCES

[1] MITRE ATT&CK: Credential Access (TA0006)

[2] HuggingFace, Agent intrusion technical timeline

[3] MITRE ATT&CK: Steal Application Access Token (T1528)

Find the exposed credentials before an attacker does.

securelayer7.net/learn/credential-access/jwt-signing-key-theft

Open online