Detection Strategy for Forged Web Credentials, Detection Strategy DET0260

Archived: 2026-04-05 17:50:05 UTC

AN0717

Defenders may detect adversaries forging web credentials in IaaS environments by monitoring for anomalous API activity such as AssumeRole or GetFederationToken being executed by unusual principals. These events often correlate with sudden logon sessions from unfamiliar IP addresses or regions. The chain is usually secret material misuse (stolen private key or password) → API request generating a new token → access to high-value resources.

Log Sources

Mutable Elements

Field	Description
AuthorizedRoleMappings	Define expected users and roles allowed to use AssumeRole or federation APIs.
GeoVelocityThreshold	Alert if the same user authenticates from geographically disparate locations within a short time.

AN0718

Forged web credentials may manifest as anomalous SAML token issuance, OpenID Connect token minting, or Zimbra pre-auth key usage. Defenders may see tokens issued without normal authentication events, multiple valid tokens generated simultaneously, or signing anomalies in IdP logs.

Log Sources

Mutable Elements

Field	Description
TokenLifetimeThreshold	Limit the maximum time temporary tokens are valid.
ExpectedAuthFlows	Define normal authentication flows (e.g., password+MFA) to baseline token issuance.

AN0719

Forged web credentials on Windows endpoints may be detected by anomalous browser cookie files, local token cache manipulations, or tools injecting tokens into sessions. Defenders may observe processes accessing LSASS or browser credential stores unexpectedly, followed by unusual logon sessions.

Log Sources

Mutable Elements

Field	Description
ProcessWhitelist	Define expected processes that access LSASS or browser credential files.

AN0720

On Linux systems, forged credentials may be injected into browser session files, curl/wget headers, or token caches in memory. Detection can leverage auditd to track processes accessing sensitive files (~/.mozilla, ~/.config/chromium, ~/.aws/credentials) and correlate with suspicious outbound connections.

Log Sources

Mutable Elements

Field	Description
CredentialFilePaths	Define which credential and session files should trigger monitoring.

AN0721

Forged credentials on macOS may be visible through Unified Logs showing abnormal access to Keychain or browser session files. Correlated with anomalous web session usage from Safari or Chrome processes outside typical user context.

Log Sources

Mutable Elements

Field	Description
AuthorizedKeychainApps	List applications that normally request Keychain credentials.

AN0722

SaaS platforms may show forged credentials as unusual API keys, tokens, or session cookies being used without corresponding authentication. Correlated patterns include simultaneous valid sessions from multiple geographies, unusual API calls with new tokens, or bypass of expected MFA enforcement.

Log Sources

Mutable Elements

Field	Description
GeoLocationAlerts	Trigger on logins from unusual or high-risk geographies.
TokenReplayThreshold	Detect multiple simultaneous uses of the same forged credential.

AN0723

Forged web credentials in Office Suite contexts may appear as abnormal authentication headers in Outlook or Teams traffic, or unexplained OAuth grants in M365/Azure logs. Defenders should correlate token usage events with missing authentication flows and mismatched device/user context.

Log Sources

Mutable Elements

Field	Description
OAuthAppAllowlist	Approved OAuth apps and flows; flag unapproved or unexpected token grants.
