Detection Strategy for Forged Web Cookies, Detection Strategy DET0171

Archived: 2026-04-05 13:50:32 UTC

AN0483

Forged cookies in IaaS environments may appear as authentication attempts that bypass MFA, leveraging AssumeRole or session APIs with cookies that were never legitimately issued. Defenders should correlate cloud logs for cookie-based sessions without prior valid authentication, often followed by resource access from unfamiliar IP addresses.

Log Sources

Mutable Elements

Field	Description
GeoVelocityThreshold	Flag logins from geographically distant locations in a short timeframe.
AuthorizedCookieIssuers	Expected systems and services that may legitimately mint session cookies.

AN0484

Forged web cookies on Windows endpoints can be detected by monitoring unusual modifications of browser cookie stores (e.g., Chrome SQLite DB, Edge cache) by processes outside of browsers, followed by authentication events to SaaS or IaaS services. Defenders may observe processes writing directly to cookie storage paths or injecting tokens into browser sessions.

Log Sources

Mutable Elements

Field	Description
BrowserCookiePaths	List of monitored cookie file paths on Windows systems.
ProcessWhitelist	Approved processes allowed to write to browser cookie stores.

AN0485

On Linux, defenders may observe forged cookie activity as unauthorized modifications to browser cookie databases (e.g., ~/.mozilla/firefox/*/cookies.sqlite, ~/.config/chromium/Default/Cookies) or scripted injection of

session tokens. Suspicious usage includes curl/wget commands embedding forged cookies in headers, correlated with abnormal session activity in SaaS or IaaS logs.

Log Sources

Mutable Elements

Field	Description
CredentialFilePaths	Paths to cookie/session storage files to monitor.

AN0486

Forged cookies on macOS may show up as abnormal access to Safari/Chrome cookie databases in ~/Library/Cookies, combined with unexpected logon sessions authenticated by those cookies. Unified Logs may show cookie injection events or abnormal access patterns to Keychain when linked to browser authentication flows.

Log Sources

Data Component	Name	Channel
File Access (DC0055)	macos:unifiedlog	Abnormal process access to Safari or Chrome cookie storage
Web Credential Usage (DC0007)	macos:unifiedlog	New session initiated using cookies without normal MFA or password validation

Mutable Elements

Field	Description
AuthorizedKeychainApps	Applications permitted to use Keychain to generate cookies or tokens.

AN0487

Forged cookies in SaaS environments manifest as valid web sessions without matching login activity, MFA enforcement bypass, or cookies reused across multiple devices/IPs. Defenders should look for cookie replay, concurrent sessions from multiple geographies, or session tokens generated by unrecognized apps.

Log Sources

Mutable Elements

Field	Description
TokenReplayThreshold	Number of concurrent uses of a cookie that should trigger an alert.
GeoLocationAlerts	Unusual SaaS logins from geographically distant locations in short timeframes.

Source: https://attack.mitre.org/detectionstrategies/DET0171#AN0483