AUT-0 · Mobile Threat Catalogue

Archived: 2026-04-05 18:13:00 UTC

Mobile Threat Catalogue

Use of Stolen Credentials

Contribute

Threat Category: Authentication: User or Device to Remote Service

ID: AUT-0

Threat Description: Attackers able to steal authorized credentials could potentially login to sensitive services or devices, and gain unauthorized access to privileged information.

Threat Origin

Mobile Threat Protection: A Holistic Approach to Securing Mobile Data and Devices [1]

Exploit Examples

CBS App & Mobility Website [2]

The Fork [3]

Star Q8 [4]

Corriere Della Sera App [5]

LaTribune [6]

Card Crypt [7]

Starbucks Caught Storing Mobile Passwords in Clear Text [8]

CVE Examples

Possible Countermeasures

Enterprise

To hinder an authentication attempt with a stolen credential, use anomaly detection based on user activity to detect abnormalities (e.g. authentication from new domains, unusual times, or to rarely-accessed services) and require additional authentication steps before granting access.

To mitigate an attacker’s ability to achieve authentication using a stolen credential, when possible, configure services to use multi-factor authentication. Ideally, the additional factor should be provided by a separate device than the one being used to perform primary authentication (e.g., laptop and mobile app). Further, avoid the use of SMS messages for 2FA codes, as SMS messages can be readily intercepted.

To limit the value of stolen credentials to an attacker, use centralized identity and access management tools that permit simultaneous revocation of stolen authentication credentials across all access control mechanisms and terminate active sessions based on those credentials.

To limit the value of stolen credentials, enforce a policy that limits the maximum age of credentials and limits the use of identical or similar credentials.

To limit the value of stolen credentials, enforce an access policy that restricts the resources a user can access based on location parameters (e.g. domain, IP address, MAC address, geolocation) of the authentication request.

Incorporate the principle of least privilege to limit lateral movement by an attacker with stolen credentials.

To limit the potential for predictive attacks on new passwords, employ authentication mechanisms that utilizes randomly generated one-time passwords or tokens for access from untrusted locations.

To prevent an attacker with a stolen password from locking out the legitimate user or defining new credentials, require 2-factor authentication mechanisms to change authentication credentials or credential recovery processes.

Mobile Device User

To mitigate an attacker’s ability to achieve authentication using a stolen credential, when possible, configure services to use multi-factor authentication. Ideally, the additional factor should be provided by a separate device than the one being used to perform primary authentication (e.g., laptop and mobile app). Further, avoid the use of SMS messages for 2FA codes, as SMS messages can be readily intercepted.

References
