Index -

Archived: 2026-04-05 17:07:52 UTC

iOS URL Scheme Hijacking

Description

The application can register URI schemes to handle actions like single-sign-on, deep application linking or to perform cross-application communication.

A malicious application can register a URI already in use by a genuine application and be able to intercept data intended for it, which can contain sensitive information like OAuth authorization codes or tokens.

Recommendation

To mitigate risk of URL scheme hijacking on iOS, it is recommended to use iOS universal links.

Universal links prevent malicious application interception through a vetting process using standard web links (HTTP/HTTPS).

For instance, the Telegram app supports both custom URL schemes and universal links:

- `tg://resolve?domain=fridadotre` is a custom URL scheme and uses the `tg://` scheme.
- `https://telegram.me/fridadotre` is a universal link and uses the `https://` scheme.

This model ensures universal links are unique, and secure without sacrificing simplicity and flexibility.

Links

- MITRE ATT&CK - URI Hijacking
- Prevent iOS URL Scheme Hijack

Standards

- OWASP_MASVS_L1:
  - MSTG_PLATFORM_3
- OWASP_MASVS_L2:
  - MSTG_PLATFORM_3
- GDPR:
  - ART_5
  - ART_32
- PCI_STANDARDS:
  - REQ_6_2

    - REQ_6_3
    - REQ_11_3
- OWASP_MASVS_v2_1:
    - MASVS_CODE_4
- SOC2_CONTROLS:
    - CC_2_1
    - CC_4_1
    - CC_7_1
    - CC_7_2
    - CC_7_4
    - CC_7_5
- CNIL_FOR_DEVELOPERS:
    - DEVELOPERS_4_1_4
- HIPAA_CONTROLS:
    - SECURITY221
    - SECURITY212
    - SECURITY213
