# MOBSF

## IOS STATIC ANALYSIS REPORT

AppGestionUAM (1.0)

| | |
|---|---|
| File Name: | AppGestionUAM.ipa |
| Identifier: | com.allwinsolutions.uam-demo-app |
| Scan Date: | Jan. 29, 2025, 5:09 p.m. |
| App Security Score: | 85/100 (LOW RISK) |
| Grade: |  |

# FINDINGS SEVERITY

| HIGH | MEDIUM | INFO | SECURE | HOTSPOT |
|---|---|---|---|---|
| 0 | 1 | 0 | 1 | 0 |

# FILE INFORMATION

**File Name:** AppGestionUAM.ipa
**Size:** 0.53MB
**MD5:** 6989636cf7af6bf5883ecfc125ffbe69
**SHA1:** 188e398565e808c03706ea2ffe651898dc86f892
**SHA256:** 7ee1978db68639097851ac2f7cb514bccefb2a92ef884a20e2ebe5eb02c878fb

# APP INFORMATION

**App Name:** AppGestionUAM
**App Type:** Swift
**Identifier:** com.allwinsolutions.uam-demo-app
**SDK Name:** iphoneos18.2
**Version:** 1.0
**Build:** 5
**Platform Version:** 18.2
**Min OS Version:** 18.0
**Supported Platforms:** iPhoneOS,

# BINARY INFORMATION

**Arch:** ARM64
**Sub Arch:** CPU_SUBTYPE_ARM64_ALL
**Bit:** 64-bit
**Endian:** <

# APP TRANSPORT SECURITY (ATS)

| NO | ISSUE | SEVERITY | DESCRIPTION |
|---|---|---|---|

# IPA BINARY CODE ANALYSIS

| NO | ISSUE | SEVERITY | STANDARDS | DESCRIPTION |
|---|---|---|---|---|

# IPA BINARY ANALYSIS

| PROTECTION | STATUS | SEVERITY | DESCRIPTION |
|---|---|---|---|
| NX | False | info | The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. However iOS never allows an app to execute from writeable memory. You do not need to specifically enable the 'NX bit' because it's always enabled for all third-party code. |

| PROTECTION | STATUS | SEVERITY | DESCRIPTION |
|---|---|---|---|
| PIE | True | info | The binary is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably. |
| STACK CANARY | True | info | This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return. |
| ARC | True | info | The binary is compiled with Automatic Reference Counting (ARC) flag. ARC is a compiler feature that provides automatic memory management of Objective-C objects and is an exploit mitigation mechanism against memory corruption vulnerabilities. |
| RPATH | True | warning | The binary has Runpath Search Path (@rpath) set. In certain cases an attacker can abuse this feature to run arbitrary executable for code execution and privilege escalation. Remove the compiler option -rpath to remove @rpath. |
| CODE SIGNATURE | True | info | This binary has a code signature. |
| ENCRYPTED | False | warning | This binary is not encrypted. |
| SYMBOLS STRIPPED | True | info | Debug Symbols are stripped |

# </> CODE ANALYSIS

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|---|---|---|---|---|

# ! OFAC SANCTIONED COUNTRIES

This app may communicate with the following OFAC sanctioned list of countries.

| DOMAIN | COUNTRY/REGION |
|---|---|

# DOMAIN MALWARE CHECK

| DOMAIN | STATUS | GEOLOCATION |
|---|---|---|
| uam-server.up.railway.app | ok | **IP:** 35.212.94.98<br>**Country:** United States of America<br>**Region:** District of Columbia<br>**City:** Washington<br>**Latitude:** 38.895111<br>**Longitude:** -77.036369<br>**View:** Google Map |
| certs.apple.com | ok | **IP:** 17.253.7.141<br>**Country:** United States of America<br>**Region:** Georgia<br>**City:** Atlanta<br>**Latitude:** 33.749001<br>**Longitude:** -84.387978<br>**View:** Google Map |

| DOMAIN | STATUS | GEOLOCATION |
| --- | --- | --- |
| crl.apple.com | ok | **IP:** 17.253.7.145<br>**Country:** United States of America<br>**Region:** Georgia<br>**City:** Atlanta<br>**Latitude:** 33.749001<br>**Longitude:** -84.387978<br>**View:** Google Map |
| www.apple.com | ok | **IP:** 23.209.221.54<br>**Country:** Indonesia<br>**Region:** Jawa Barat<br>**City:** Ancol<br>**Latitude:** -7.365100<br>**Longitude:** 108.387100<br>**View:** Google Map |
| ocsp.apple.com | ok | **IP:** 23.197.168.157<br>**Country:** Korea (Republic of)<br>**Region:** Seoul-teukbyeolsi<br>**City:** Seoul<br>**Latitude:** 37.568260<br>**Longitude:** 126.977829<br>**View:** Google Map |

## SCAN LOGS

| Timestamp | Event | Error |
| --- | --- | --- |
| 2025-01-29 17:09:17 | iOS Binary (IPA) Analysis Started | OK |

| | | |
|---|---|---|
| 2025-01-29 17:09:17 | Generating Hashes | OK |
| 2025-01-29 17:09:17 | Extracting IPA | OK |
| 2025-01-29 17:09:17 | Unzipping | OK |
| 2025-01-29 17:09:17 | iOS File Analysis and Normalization | OK |
| 2025-01-29 17:09:17 | iOS Info.plist Analysis Started | OK |
| 2025-01-29 17:09:17 | Finding Info.plist in iOS Binary | OK |
| 2025-01-29 17:09:17 | Fetching Details from App Store: com.allwinsolutions.uam-demo-app | OK |
| 2025-01-29 17:09:17 | Searching for secrets in plist files | OK |
| 2025-01-29 17:09:17 | Starting Binary Analysis | OK |
| 2025-01-29 17:09:17 | Dumping Classes from the binary | OK |

| | | |
|---|---|---|
| 2025-01-29 17:09:17 | Running jtool against the binary for dumping classes | OK |
| 2025-01-29 17:09:17 | Library Binary Analysis Started | OK |
| 2025-01-29 17:09:17 | Framework Binary Analysis Started | OK |
| 2025-01-29 17:09:17 | Extracting String Metadata | OK |
| 2025-01-29 17:09:17 | Extracting URL and Email from IPA | OK |
| 2025-01-29 17:09:17 | Performing Malware check on extracted domains | OK |
| 2025-01-29 17:09:19 | Fetching IPA icon path | OK |
| 2025-01-29 17:09:21 | Detecting Trackers from Domains | OK |
| 2025-01-29 17:09:21 | Updating Database... | OK |

---

## Report Generated by - MobSF v4.3.0

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.