

Secsys-FDU / AF_CVEs Public

[Code](#) [Issues 27](#) [Pull requests](#) [Actions](#) [Projects](#) [Security and quality](#)

New issue



Video player - Play All Videos APP Arbitrary File Overwrite Vulnerability #29

Open



Secsys-FDU opened 16 hours ago

Owner



Vendor : RAREPROB SOLUTIONS PRIVATE LIMITED(<https://rareprob-website.firebaseio.com/>)

Affected product : Video player - Play All Videos (rocks.video.videoplayer)

Version : V1.0.135

Google Play link : <https://play.google.com/store/apps/details?id=rocks.video.videoplayer>

Description of the vulnerability for use in the CVE : An arbitrary file overwrite vulnerability in the Video player - Play All Videos app allows attackers to overwrite critical internal files via the file import process, potentially enabling code execution, exposure of sensitive information, denial of service, and other severe security impacts.

Vulnerability Component : com.kaisquare.location.MainActivity

Additional information : This vulnerability is caused by insufficient security validation when handling imported files. A malicious app can control the filename and content and use path traversal to overwrite sensitive files in the app's internal storage. When critical configuration or executable files are modified, the app may malfunction, fail to launch, or execute arbitrary code. The attack requires no complex user interaction and can be triggered automatically once the victim opens the malicious app.

Before Overwrite:

```

panther:/data/data/rocks.video.videoplayer/shared_prefs # ls -al
total 142
drwxrwx--x  2 u0_a686 u0_a686 3452 2026-01-29 16:35 .
drwx----- 13 u0_a686 u0_a686 3452 2026-01-29 16:26 ..
-rw-rw----  1 u0_a686 u0_a686  431 2026-01-29 16:29 AwOriginVisitLoggerPrefs.xml
-rw-rw----  1 u0_a686 u0_a686  110 2026-01-29 16:31 DEBUG_PREF.xml
-rw-rw----  1 u0_a686 u0_a686  415 2026-01-29 16:35 FBAdPrefs.xml
-rw-rw----  1 u0_a686 u0_a686  670 2026-01-29 16:29 FirebasePerfSharedPrefs.xml
-rw-rw----  1 u0_a686 u0_a686  127 2026-01-29 16:19 WebViewChromiumPrefs.xml
-rw-rw----  1 u0_a686 u0_a686 1082 2026-01-29 16:26 __GOOGLE_FUNDING_CHOICE_SDK_INTERNAL__.xml
-rw-rw----  1 u0_a686 u0_a686 17766 2026-01-29 16:31 admob.xml
-rw-rw----  1 u0_a686 u0_a686  281 2026-01-29 16:19 admob_user_agent.xml
-rw-rw----  1 u0_a686 u0_a686  281 2026-01-29 16:26 app_set_id_storage.xml
-rw-rw----  1 u0_a686 u0_a686 4303 2026-01-29 16:26 com.facebook.ads.FEATURE_CONFIG.xml
-rw-rw----  1 u0_a686 u0_a686   65 2026-01-29 16:26 com.facebook.ads.flash.xml
-rw-rw----  1 u0_a686 u0_a686  254 2026-01-29 16:35 com.facebook.ads.internal.btextras.xml
-rw-rw----  1 u0_a686 u0_a686  252 2026-01-29 16:29 com.google.android.gms.appid.xml
-rw-rw----  1 u0_a686 u0_a686 1118 2026-01-29 16:35 com.google.android.gms.measurement.prefs.xml
-rw-rw----  1 u0_a686 u0_a686  409 2026-01-29 16:26 com.google.firebase.crashlytics.xml
-rw-rw----  1 u0_a686 u0_a686  170 2026-01-29 16:31 com.google.firebase.inappmessaging.xml
-rw-rw----  1 u0_a686 u0_a686  137 2026-01-29 16:19 com.google.firebase.messaging.xml
-rw-rw----  1 u0_a686 u0_a686  793 2026-01-29 16:29 com.music.rockes.xml
-rw-rw----  1 u0_a686 u0_a686  557 2026-01-29 16:26 frc_1:780874919150:android:9cae2e8486e62ddd53d7ff_firebase_settings.xml
-rw-rw----  1 u0_a686 u0_a686  434 2026-01-29 16:27 frc_1:780874919150:android:9cae2e8486e62ddd53d7ff_fireperf_settings.xml
-rw-rw----  1 u0_a686 u0_a686 5060 2026-01-29 16:26 pag_adn_strategy_center.xml
-rw-rw----  1 u0_a686 u0_a686  129 2026-01-29 16:26 pag_monitor_record.xml
-rw-rw----  1 u0_a686 u0_a686  958 2026-01-29 16:29 pag_sp_bad_par.xml
-rw-rw----  1 u0_a686 u0_a686  117 2026-01-29 16:26 pag_sp_prop_switch.xml
-rw-rw----  1 u0_a686 u0_a686  346 2026-01-29 16:26 paid_storage_sp.xml
-rw-rw----  1 u0_a686 u0_a686  706 2026-01-29 16:26 rocks.video.videoplayer_preferences.xml
-rw-rw----  1 u0_a686 u0_a686  802 2026-01-29 16:26 ss_config.xml
-rw-rw----  1 u0_a686 u0_a686   65 2026-01-29 16:26 tt_sdk_settings.xml
panther:/data/data/rocks.video.videoplayer/shared_prefs # cat paid_storage_sp.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
  <long name="paidv1_creation_time" value="1769675151" />
  <long name="paidv2_creation_time" value="1769675195" />
  <string name="paidv2_id">126ca0fe-9fa2-4d92-8689-4322e83117766</string>
  <string name="paidv1_id">f2e0a86e-7b1e-4a56-bc2a-e742917766</string>
</map>

```

After Overwrite:

```

panther:/data/data/rocks.video.videoplayer/shared_prefs # ls -al
total 142
drwxrwx--x  2 u0_a686 u0_a686 3452 2026-01-29 16:39 .
drwx----- 13 u0_a686 u0_a686 3452 2026-01-29 16:26 ..
-rw-rw----  1 u0_a686 u0_a686  431 2026-01-29 16:29 AwOriginVisitLoggerPrefs.xml
-rw-rw----  1 u0_a686 u0_a686  110 2026-01-29 16:31 DEBUG_PREF.xml
-rw-rw----  1 u0_a686 u0_a686  415 2026-01-29 16:35 FBAdPrefs.xml
-rw-rw----  1 u0_a686 u0_a686  670 2026-01-29 16:29 FirebasePerfSharedPrefs.xml
-rw-rw----  1 u0_a686 u0_a686  127 2026-01-29 16:19 WebViewChromiumPrefs.xml
-rw-rw----  1 u0_a686 u0_a686 1082 2026-01-29 16:26 __GOOGLE_FUNDING_CHOICE_SDK_INTERNAL__.xml
-rw-rw----  1 u0_a686 u0_a686 17766 2026-01-29 16:39 admob.xml
-rw-rw----  1 u0_a686 u0_a686  281 2026-01-29 16:19 admob_user_agent.xml
-rw-rw----  1 u0_a686 u0_a686  281 2026-01-29 16:26 app_set_id_storage.xml
-rw-rw----  1 u0_a686 u0_a686 4303 2026-01-29 16:26 com.facebook.ads.FEATURE_CONFIG.xml
-rw-rw----  1 u0_a686 u0_a686   65 2026-01-29 16:26 com.facebook.ads.flash.xml
-rw-rw----  1 u0_a686 u0_a686  254 2026-01-29 16:35 com.facebook.ads.internal.btextras.xml
-rw-rw----  1 u0_a686 u0_a686  252 2026-01-29 16:29 com.google.android.gms.appid.xml
-rw-rw----  1 u0_a686 u0_a686 1118 2026-01-29 16:39 com.google.android.gms.measurement.prefs.xml
-rw-rw----  1 u0_a686 u0_a686  409 2026-01-29 16:26 com.google.firebase.crashlytics.xml
-rw-rw----  1 u0_a686 u0_a686  170 2026-01-29 16:31 com.google.firebase.inappmessaging.xml
-rw-rw----  1 u0_a686 u0_a686  137 2026-01-29 16:19 com.google.firebase.messaging.xml
-rw-rw----  1 u0_a686 u0_a686  848 2026-01-29 16:39 com.music.rockes.xml
-rw-rw----  1 u0_a686 u0_a686  557 2026-01-29 16:26 frc_1:780874919150:android:9cae2e8486e62ddd53d7ff_firebase_settings.xml
-rw-rw----  1 u0_a686 u0_a686  434 2026-01-29 16:27 frc_1:780874919150:android:9cae2e8486e62ddd53d7ff_fireperf_settings.xml
-rw-rw----  1 u0_a686 u0_a686 5060 2026-01-29 16:26 pag_adn_strategy_center.xml
-rw-rw----  1 u0_a686 u0_a686  129 2026-01-29 16:26 pag_monitor_record.xml
-rw-rw----  1 u0_a686 u0_a686  958 2026-01-29 16:29 pag_sp_bad_par.xml
-rw-rw----  1 u0_a686 u0_a686  117 2026-01-29 16:26 pag_sp_prop_switch.xml
-rw-rw----  1 u0_a686 u0_a686  18 2026-01-29 16:39 paid_storage_sp.xml
-rw-rw----  1 u0_a686 u0_a686  706 2026-01-29 16:26 rocks.video.videoplayer_preferences.xml
-rw-rw----  1 u0_a686 u0_a686  802 2026-01-29 16:26 ss_config.xml
-rw-rw----  1 u0_a686 u0_a686   65 2026-01-29 16:26 tt_sdk_settings.xml
panther:/data/data/rocks.video.videoplayer/shared_prefs # cat paid_storage_sp.xml
<b>Attack@Test</b>panther:/data/data/rocks.video.videoplayer/shared_prefs #

```

[Sign up for free](#) to join this conversation on **GitHub**. Already have an account? [Sign in to comment](#)

Metadata

Assignees

No one assigned

Labels

No labels

Projects

No projects


Milestone

No milestone

Relationships

None yet

Development

 Code with agent mode

No branches or pull requests

Participants

