New issue

Voice Recorder APP Arbitrary File Overwrite and Read Vulnerability #25

Open

Secsys-FDU opened 13 hours ago Owner

Vendor：UXGROUP LLC(https://appcraze.co/)

Affected product：Voice Recorder (ac.voicenote.voicerecorder.audio)

Version：V10.0

Google Play link：https://play.google.com/store/apps/details?id=ac.voicenote.voicerecorder.audio

Description of the vulnerability for use in the CVE：An arbitrary file overwrite vulnerability in the Voice Recorder app allows attackers to overwrite critical internal files via the file import process, potentially leading to code execution, sensitive information disclosure, denial of service, and other severe security impacts. In addition, an arbitrary file read vulnerability enables attackers to access sensitive internal files after user login, including authentication state and session-related data. When these two vulnerabilities are combined, they may further lead to account hijacking, configuration tampering, persistent compromise of the application, and other serious security consequences.

Vulnerability Component：com.kyungeun.timer.activities.overloads.PlayRecordingActivity

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 and read sensitive files in the app’s internal storage. When critical configuration or executable files are modified or read, 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.

An attacker can control the victim application to write sensitive files to shared storage, resulting in data leakage. For example, com.google.android.gms.signin.xml contains user login information, which could potentially lead to account hijacking.

```
OP5D0DL1:/data/data/ac.voicenote.voicerecorder.audio/shared_prefs # ls
AwOriginVisitLoggerPrefs.xml
DEBUG_PREF.xml
FBAdPrefs.xml
FirebaseHeartBeatW0RFRkFVTFRd+MToxMDk0MTc1MzE3NTQ0OmFuZHJvaWQ6NzM3MDZiMWQwNTQxN
MyPrefs.xml
Prefs.xml
WebViewChromiumPrefs.xml
__GOOGLE_FUNDING_CHOICE_SDK_INTERNAL__.xml
ac.voicenote.voicerecorder.audio_preferences.xml
admob.xml
appOpenAdsManager.xml
com.facebook.ads.FEATURE_CONFIG.xml
com.facebook.ads.LOCAL_COUNTERS.xml
com.facebook.ads.flash.xml
com.facebook.ads.idfa.xml
com.facebook.ads.internal.btextras.xml
com.google.android.gms.measurement.prefs.xml
com.google.android.gms.signin.xml
com.google.firebase.crashlytics.xml
frc_1:1094175317544:android:73706b1d05417ea4135f1d_firebase_settings.xml
pag_adn_strategy_center.xml
pag_monitor_record.xml
pag_sp_bad_par.xml
pag_sp_prop_switch.xml
paid_storage_sp.xml
pcvmspf.xml
ss_config.xml
tt_sdk_settings.xml
```

Sensitive files exported to shared storage; in addition, an attacker can also overwrite sensitive files within the application.

```
OP5D0DL1:/sdcard/Documents # cat dump_siginin_file
cat: dump_siginin_file: No such file or directory
1|OP5D0DL1:/sdcard/Documents # cat dump_siginin_file
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <string name="googleSignInAccount [redacted]>{&quot;id&quot;:&quot [redacted]
1&quot;,&quot;email&quot;:&quot [redacted] @gmail.com&quot;,&quot;displayName&quot;:&quot [redacted] &quot;,&quot;givenN
ame&quot;:&quot [redacted] &quot;,&quot;expirationTime&quot;:1769694769,&quot;obfuscatedIdentifier&quot;:&quot [redacted]
[redacted] :,&quot;grantedScopes&quot;:[&quot;email&quot;,&quot;https:\/\/www.googleapis.com\/au
th\/drive.file&quot;,&quot;https:\/\/www.googleapis.com\/auth\/userinfo.email&quot;,&quot;https:\/\/www.googleapis
.com\/auth\/userinfo.profile&quot;,&quot;openid&quot;,&quot;profile&quot;]}</string>
    <string name="googleSignInOptions [redacted] &quot;scopes&quot;:[&quot;email&quot;,&qu
ot;https:\/\/www.googleapis.com\/auth\/drive.file&quot;,&quot;openid&quot;,&quot;profile&quot;],&quot;idTokenReque
sted&quot;:false,&quot;forceCodeForRefreshToken&quot;:false,&quot;serverAuthRequested&quot;:false}</string>
    <string name="defaultGoogleSignInAccount" [redacted] /string>
</map>
```


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