New issue

Zora: Post, Trade, Earn Crypto APP Arbitrary File Overwrite Vulnerability #15

Open

Secsys-FDU opened 17 hours ago Owner

Vendor：Zora Labs, Inc(https://zora.co/)

Affected product：Zora: Post, Trade, Earn Crypto (co.ourzora.app), https://play.google.com/store/apps/details?id=co.ourzora.app

Version：2.60.0

Google Play link：https://play.google.com/store/apps/details?id=co.ourzora.app

Description of the vulnerability for use in the CVE：An arbitrary file overwrite vulnerability in the Zora: Post, Trade, Earn Crypto 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：co.ourzora.app.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:

```
OP5D0DL1:/data/data/co.ourzora.app/shared_prefs # ls
AwOriginVisitLoggerPrefs.xml
FirebaseHeartBeatW0RFRkFVTFRd+MTo5ODg1NzgwMTQ3MDM6YW5kcm9pZDo3ZDIzNDE0MjI1NzliMmUzM2UwMjFh.xml
SecureStore.xml
WebViewChromiumPrefs.xml
analytics-android-10a2d59ed7ccbc13024a.xml
appsflyer-data.xml
com.google.android.gms.appid.xml
com.google.firebase.messaging.xml
dev.expo.EASSharedPreferences.xml
expo.modules.kotlin.PersistentDataManager.xml
io.customer.sdk.co.ourzora.app.xml
OP5D0DL1:/data/data/co.ourzora.app/shared_prefs # cat SecureStore.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <string name="key_v1-privy-token">{&quot;ct&quot;:&quot;THg1espeqq\/lRqK[redacted]LiuNz32
GoT6PrDwbVuzNRnfvBnMY8oMsammI1UyR61xz0umALE\/etco8ScuvPxKJkXcdPGHM7JbCME1iNq16Ate1n\/[redacted]GHrvfcrBA
LzTUcpt9tw71AyFQDGLgSmpfCWv4Jy[redacted]XflvJB1i\/tIHns
+rbkqPK6UrtuXvjGNGA5\/DiR\/yNdxKkf\/NmYKK6[redacted]qcCXv
n05jRU6Fc0kscnzSz+qibNxwxkXE8gN6FAo9FBXoPUamTkB\/TVTA6TA9FaPpj3WOKYWWiV44Z4ODEYWDYNyFGAicqhvKoWfm4e&quot;,&quot;iv&quot;:&quot;d25JriyGA
T2YJf9G&quot;,&quot;tlen&quot;:128,&quot;scheme&quot;:&quot;aes&quot;,&quot;usesKeystoreSuffix&quot;:true,&quot;keystoreAlias&quot;:&quo
t;key_v1&quot;,&quot;requireAuthentication&quot;:false}</string>
    <string name="key_v1-privy-__storage__test-03a46d55-f13a-412d-a[redacted];:&quot;KrF3GKTRfn0Y3MFxdPCE1xeEcXz4p
g==&quot;,&quot;iv&quot;:&quot;uNs0a8iRSy6[redacted]&quot;tlen&quot;:128,&quot;scheme&quot;:&quot;aes&quot;,&quot;usesKeystoreSuffix&q
uot;:true,&quot;keystoreAlias&quot;:&quot;key_v1[redacted]uthentication&quot;:false[redacted]
    <string name="key_v1-privy-refresh_token">{&quot;ct&quot;:&quot;wF6FUFj0x3X7pUPWxs5o8mSgT[redacted]eUVYn+
4SplpCsj[redacted]&quot;,&quot;iv&quot;:&quot;m5+fhx\/lszc44hsE&quot;,&quot;tlen&quot
;:128,&quot;scheme&quot;:&quot;aes&quot;,&quot;usesKeystoreSuffix&quot;:true,&quot;keystoreAlias&quot;:&quot;key_v1&quot;,&quot;requireA
uthentication&quot;:false}</string>
    <string name="key_v1-privy-caid">{&quot;ct&quot[redacted]
t;,&quot;iv&quot;:[redacted]tlen&quot;:128,&quot;scheme&quot;:&quot;aes&quot;,&quot;usesKeystoreSuffix&quot;:tr
ue,&quot;keystoreAlias&quot;:&quot;key_v1&quot;,&quot;requireAuthentication&quot;:false}</string>
</map>
```

After Overwrite:

```
OP5D0DL1:/data/data/co.ourzora.app/shared_prefs # cat SecureStore.xml
<b>Attack@Test</b>OP5D0DL1:/data/data/co.ourzora.app/shared_prefs #
```

By overwriting executable files, an attacker can achieve arbitrary code execution, or overwrite critical configuration files to perform privilege escalation.

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