New issue

InTouch Contacts & Caller ID APP Arbitrary File Overwrite Vulnerability #19

Open

Secsys-FDU opened 4 days ago Owner

Vendor：InTouchApp(https://www.intouchapp.com/)

Affected product：InTouch Contacts & Caller ID APP (net.IntouchApp), https://play.google.com/store/apps/details?id=net.IntouchApp

Version：6.38.1

Google Play link：https://play.google.com/store/apps/details?id=net.IntouchApp

Description of the vulnerability for use in the CVE：An arbitrary file overwrite vulnerability in the InTouch Contacts 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.intouchapp.activities.ext_share.ExternalShareActivity

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/net.IntouchApp/shared_prefs # cat com.google.android.gms.appid.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <string name="|T|233242896108|*">{&amp;quot;token&amp;quot;:&amp;quot;cSHL8Fm6RWmOC63lXwpx-L:APA91bGTFK7LvUsaoIyxMMSg1prm7YZHfOjr3WNDFJbK9AGk-R1uhRw1zDqBpPUyxr
I20mWlh5JQFmve7aXFEN6EVWOVY0GWtyDmXuyO7R38KQsbLU3_EYU&amp;quot;,&amp;quot;appVersion&amp;quot;:&amp;quot;2026012101&amp;quot;,&amp;quot;timestamp&amp;quot;:1770004479712}</string>
</map>
```

After Overwrite:

```
OP5D0DL1:/data/data/net.IntouchApp/shared_prefs # cat com.google.android.gms.appid.xml
<b>Attack@Test</b>OP5D0DL1:/data/data/net.IntouchApp/shared_prefs #
```

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

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