

## **U4I: Actions Taken to Address Findings and Recommendations from the Second Pentest-Report**

According to the second round of penetration testing done by Cure53, following issues have been flagged.

- [U4I-06-002 Android: DoS via intent to ImportTextActivity \(Medium\)](#)
- [U4I-06-003 Android: DoS via intent to ImportImageActivity \(Medium\)](#)
- [U4I-06-004 Android: DoS via intent to LoginActivity \(Medium\)](#)
- [U4I-06-005 Android: Passcode bypass allows message decryption \(Critical\)](#)
- [U4I-06-001 Android: General hardening recommendations for Android app \(Info\) Conclusions](#)

U4I's in-house development team reviewed the [source code](#) provided by the [Operator Foundation](#), and have concluded that all the findings have been addressed and the recommendations were adopted. We have verified this claim by reviewing the [code on GitHub](#).

Please note that only one of the findings was marked as critical. For addressing that issue, "U4I-06-005 Android: Passcode bypass allows message decryption" there is a commit on Github with the same title number U4I-06-005. U4I's in-house development team has verified that the developers of Operator Foundation added an "unregister receiver" which has resolved the issue.

Other fixes and changes to address the three medium-criticality findings and "general hardening recommendations" are also marked in the code with their respective finding code in the report (see below screenshots):

## U4I-06-002 Android: DoS via Intent to ImportTextActivity (Medium) U4I...

[Browse files](#)

...-06-003 Android: DoS via Intent to ImportImageActivity (Medium)

main

Jessica9-star committed on Jul 16

1 parent 6fc9102

commit a3b7929331a5d7929103635a2faad3c83825a344

Showing 2 changed files with 26 additions and 13 deletions.


[Unified](#)[Split](#)

19 app/src/main/java/org/naht/Nahoft/activities/ImportImageActivity.kt

```
@@ -56,16 +56,23 @@ class ImportImageActivity: AppCompatActivity(), OnItemSelectedListener
56      56          addAction(LOGOUT_TIMER_VAL)
57      57      })
58      58
59      -        // Check to see if a friend was selected in a previous activity
60      -        val maybeSerializable = intent.getSerializableExtra(RequestCodes.friendExtraTaskDescription)
61      -        if (maybeSerializable != null)
62      +        try
63      +        {
64      -            val maybeFriend = maybeSerializable as? Friend
65      -            if (maybeFriend != null)
66      +            // Check to see if a friend was selected in a previous activity
67      +            val maybeSerializable = intent.getSerializableExtra(RequestCodes.friendExtraTaskDescription)
68      +            if (maybeSerializable != null)
69      +            {
70      -                sender = maybeFriend
71      -                val maybeFriend = maybeSerializable as? Friend
72      -                if (maybeFriend != null)
73      -                {
74      -                    sender = maybeFriend
75      -                }
76      +                catch (error: Exception)
77      +                {
78      +                    // Invalid data
79      +                }
80      +            import_image_button.setOnClickListener {
81      +                handleImageImport()
82      +            }
83      +        }
84      +    }
85      +}
```

Commits on Jul 20, 2021

**U4I-06-005 Android: Passcode Bypass allows Message Decryption (Critical)**

 **consuelita** committed on Jul 20




373b80c



Commits on Jul 16, 2021

**U4I-06-002 Android: DoS via Intent to ImportTextActivity (Medium) U4I...** ...


 **Jessica9-star** committed on Jul 16



a3b7929



**U4I-06-001 Android: General hardening recommendations for Android app** ...

 **Jessica9-star** committed on Jul 16



6fc9102



**Merge branch 'main' of <https://github.com/OperatorFoundation/Nahoft> i...** ...

 **consuelita** committed on Jul 16



4cac7f5



**U4I-06-002 - U4I-06-004 Android: DoS via Intent**

 **consuelita** committed on Jul 16




bd3d719



Commits on Jul 15, 2021

**U4I-06-005 Android: PIN Code Bypass allows Message Decryption**

 **Jessica9-star** committed on Jul 15



0784e53

