

New issue

[Jump to bottom](#)

fix buffer overflow in mifare ul load #1697

Merged

skotopes merged 2 commits into `flipperdevices:dev` from `VVX7:mifare_ul_buffer_overflow` on Sep 5

Conversation 2

Commits 2

Checks 8

Files changed 1



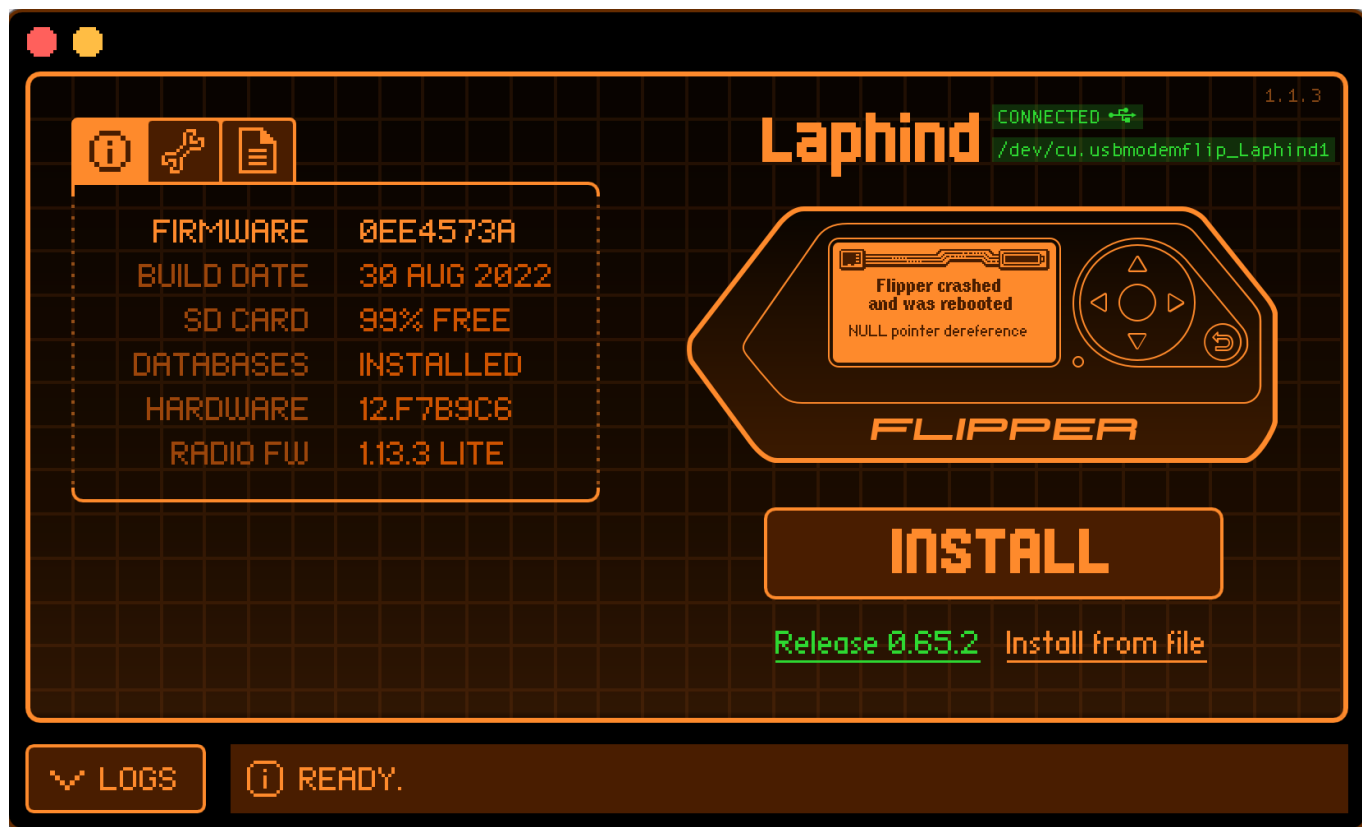
VVX7 commented on Sep 2 • edited by skotopes

Contributor

What's new

A buffer overflow exists in `nfc_device_load_mifare_ul_data` when the `pages_total` value is greater than `MF_UL_MAX_DUMP_SIZE`. This occurs because `pages_total` is parsed from the nfc file and not checked against the max size of the buffer. An nfc file with a page count greater than 2040 will result in an out of bounds write.

This may result in various crashes including a BusFault crash, and a NULL point exception. In some cases, this require re-flashing flipper firmware to recover the device :(



Shout out to <https://tmpout.sh/bggp/3/> for giving me a reason to look for bugs!! Maybe more to come ;)

Verification

Upload an nfc file containing more than 2040 pages. An example file (that will produce a null pointer deference) is provided here:

<https://gist.github.com/VVX7/c55b122846253e12f1647e2a85ab2775>

Steps:

- Upload the nfc file
- Navigate to saved nfc submenu and load the file
- view file info to trigger the crash

Note:

Larger files will result in similar unexpected behaviour and may not require viewing file info to trigger crash.

Impact

An attacker could place a malicious Amiibo file in a repository like this:

<https://github.com/Gioman101/FlipperAmiibo/>

Checklist (For Reviewer)

- ✓ PR has description of feature/bug or link to Confluence/Jira task
- ✓ Description contains actions to verify feature/bugfix
- ✓ I've built this code, uploaded it to the device and verified feature/bugfix

🔗  fix buffer overflow in mifare ul load

● e77bf96

👁  VVX7 requested review from **skotopes**, **DrZlo13**, **hedger** and **gornekich** as code owners 3 months ago

gornekich commented on Sep 2

Contributor

Hello @VVX7 . Am I right that there is no actual NFC tag with so many pages? This file was made by hands?

VVX7 commented on Sep 2

Contributor

Author

hiya @gornekich , that's right. The file was made by hand. The risk comes from someone inserting a malicious file into database of Amiibos or something similar as I linked above.

Might also be able to emulate an NFC with unusually high page count using a proxmark or hydrabus, idk. I should go poke at that...

🔗  Merge branch 'dev' into mifare_ul_buffer_overflow

✓ c329926

gornekich approved these changes on Sep 5

[View changes](#)

 skotopes merged commit **8d8481b** into [flipperdevices:dev](#) on Sep 5
8 checks passed

[View details](#)

🔗  VVX7 deleted the mifare_ul_buffer_overflow branch 3 months ago

🔗 **hedger** pushed a commit that referenced this pull request on Sep 5

 fix buffer overflow in mifare ul load ([#1697](#)) ...

40bc8be


🔗 **Dig03** pushed a commit to Dig03/flipperzero-firmware that referenced this pull request on Sep 6

 fix buffer overflow in mifare ul load ([flipperdevices#1697](#)) ...

74a46f8


 **litui** pushed a commit to litui/flipperzero-firmware that referenced this pull request on Sep 10

 fix buffer overflow in mifar ul load ([flipperdevices#1697](#)) ... ce6f8e5

 **qistoph** pushed a commit to qistoph/flipperzero-firmware that referenced this pull request on Oct 11

 fix buffer overflow in mifar ul load ([flipperdevices#1697](#)) ... 689547f

Reviewers

 gornekich	 
 skotopes	 
 DrZlo13	 
 hedger	 

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

3 participants

