New issue

Jump to bottom

Update TP-Link AC1750 Pwn2Own 2019 module #14365

Merged timwr merged 1 commit into rapid7:master from pedrib:archer_update on Nov 26, 2020

Conversation 12 Commits 1 Checks 0 Files changed 2

pedrib commented on Nov 8, 2020 • edited — Contributor

This PR updates the TP-Link AC1750 Pwn2Own Tokyo 2019 module to slightly modify the injection technique.

The new modified technique allows bypass of a patch that TP-Link issued in early 2020. The vulnerability was discovered and intended to be used in Pwn2Own Tokyo 2020, but they smartened up and patched it (this time for good) just a few days ago in the latest firmware.

The module now works on both old and new firmware up to the patched version, and also improves firmware version detection for both the A7 and C7 routers.

For more details please see: https://github.com/pedrib/PoC/blob/master/advisories/Pwn2Own/Tokyo_2020/minesweeper.md

🎉 4 ❤️ 1

pedrib commented on Nov 8, 2020 — Contributor Author

I have requested a CVE number from MITRE for the bypass and will post here as soon as I get it. Otherwise, the module is good to go, as you can see besides the check the changes are minimal, and I have tested in both A7 and C7 versions, odl and new firmware.

cdelafuente-r7 added docs module labels on Nov 16, 2020

pedrib commented on Nov 18, 2020 — Contributor Author

yello this is good to go!

I'll promise I'll deal with #14206 straight after this :D

timwr approved these changes on Nov 25, 2020

View changes

timwr left a comment — Contributor

@pedrib this looks OK to land.
Would you mind re-basing onto master and squashing it into single commit?
In theory I can do that for you...

pedrib commented on Nov 26, 2020 — Contributor Author

@timwr I'm a git noob, how do I do that?

😄 1

timwr commented on Nov 26, 2020 — Contributor

On the command line: `git rebase -i e33f4ea63e` then in the editor window do:

```
pick 019ab9aea6 Update docs
s 89b53c689f Update tplink_archer_a7_c7_lan_rce.rb
s a35465c4e0 Add new advisory links
s 0148b93752 fix typo
s 2755660a9c Update tplink_archer_a7_c7_lan_rce.md
s ee0cbd45b7 Add fixed fw version
s 03b49cf203 Update tplink_archer_a7_c7_lan_rce.md
s 0993248bdc Add new CVE ID
```

to squash all the commits into one.

Alternatively you can just do:

```
git reset --soft e33f4ea63e
git commit -m "Update TP-Link AC1750 Pwn2Own 2019 module"
```

Then just force push: `git push pedrib archer_update -f`

pedrib commented on Nov 26, 2020 — Contributor Author

I think that's done? Hope I didn't destroy anything, let me know!

timwr commented on Nov 26, 2020 — Contributor

Actually I think you just added 2 more commits rather than squashing the existing ones

1

pedrib commented on Nov 26, 2020 — Contributor, Author

Jebus, what a noob... do you mind squashing it for me? I think some of your guys were able to do that before.

`Update TP-Link AC1750 Pwn2Own 2019 module` ✕ `a99ce58`

timwr force-pushed the `archer_update` branch from **`01643ef`** to **`a99ce58`** 2 years ago — Compare

timwr commented on Nov 26, 2020 — Contributor

I pushed it but now it shows us both in the commit, I hope that's OK.
If so I'll go ahead and land it

pedrib commented on Nov 26, 2020 — Contributor, Author

of course, thank you!

timwr merged commit **`87eba68`** into `rapid7:master` on Nov 26, 2020 — View details
2 of 3 checks passed

---

timwr commented on Nov 26, 2020 • edited by pbarry-r7 — Contributor

Original Release notes

This PR updates the TP-Link AC1750 Pwn2Own Tokyo 2019 module to slightly modify the injection technique.
The new modified technique allows bypass of a patch that TP-Link issued in early 2020. The vulnerability was discovered and intended to be used in Pwn2Own Tokyo 2020, but they smartened up and patched it (this time for good) just a few days ago in the latest firmware.
The module now works on both old and new firmware up to the patched version, and also improves firmware version detection for both the A7 and C7 routers.

pedrib deleted the `archer_update` branch 2 years ago

pbarry-r7 added enhancement **rn-enhancement** labels on Dec 8, 2020

pbarry-r7 commented on Dec 9, 2020 — Contributor

Release Notes

Updated the `exploits/linux/misc/tplink_archer_a7_c7_lan_rce` module (a.k.a. TP-Link AC1750 Pwn2Own 2019) with the additional ability to bypass a patch TP-Link issued in early 2020.

Reviewers
timwr ✓

Assignees
No one assigned

Labels
docs enhancement **module** **rn-enhancement**

Projects
None yet

Milestone
No milestone

Development
Successfully merging this pull request may close these issues.
None yet

4 participants