New issue

Jump to bottom

Fix qpress directory traversal vulnerability #6

Merged PierreLvx merged 1 commit into PierreLvx:master from Chaloff:github_trversalf_fix on Aug 19

Conversation 3 Commits 1 Checks 0 Files changed 1

Chaloff commented on Aug 18 Contributor

A bad actor user can prepare the payload as:

```
mkdir -p AAAAAAAAA/secure_file_priv_dir
touch AAAAAAAAA/secure_file_priv_dir/evil.so
qpress -r AAAAAAAAA payload.qp
Then edit the payload.qp in a hex editor or sed to replace AAAAAAAAA with ../../../
(example: sed -i 's/AAAAAAAAA/..\/..\/..\//' payload.qp)
```

Fix bug by checking the directory and reject the command if find the attempt to traversal

Test: see example above and try to reproduce it. Before fix you can observe traversal. After fix - the error message(File path contains directory traversal which is not allowed.) shown, no traversal observe.

All new code of the whole pull request, including one or several files that are either new files or modified ones, are contributed under the BSD-new license. I am contributing on behalf of my employer Amazon Web Services, Inc.

Fix qpress directory traversal vulnerability ··· 02a79a7

ottok mentioned this pull request on Aug 19

PXB-2854 - Quicklz decompression memory corruption issue fix percona/percona-xtrabackup#1366

Open

PierreLvx commented on Aug 19 Owner

Thank you!

PierreLvx merged commit **ddb3120** into PierreLvx:master on Aug 19

ottok commented on Aug 19

Thanks for merging. Did you edit the commit before merging? It is no longer identical with our submission. Relevant fields such as author was changed.

This PR https://patch-diff.githubusercontent.com/raw/PierreLvx/qpress/pull/6.patch and merged commit https://github.com/PierreLvx/qpress/commit/ddb312090ebd5794e81bc6fb1dfb4e79eda48761.patch differ.

1

PierreLvx commented on Aug 19 Owner

I used Github's online interface to perform the merge.

It automatically edited the author (without any notice) and message but the code is unchanged. See:

```
➜  ~ diff 6.patch ddb312090ebd5794e81bc6fb1dfb4e79eda48761.patch
1,4c1,4
< From 02a79a793f56e86e2014a606647b158b246811e3 Mon Sep 17 00:00:00 2001
< From: Mikhail Chalov <mcchalov@amazon.com>
< Date: Wed, 14 Jul 2021 09:35:58 +0200
< Subject: [PATCH] Fix qpress directory traversal vulnerability
---
> From ddb312090ebd5794e81bc6fb1dfb4e79eda48761 Mon Sep 17 00:00:00 2001
> From: Mikhail Chalov <mike.chalov@gmail.com>
> Date: Fri, 19 Aug 2022 14:33:18 -0700
> Subject: [PATCH] Fix qpress directory traversal vulnerability (#6)
25a26,27
>
> Co-authored-by: Mikhail Chalov <mcchalov@amazon.com>
```

Reviewers

No reviews

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