New issue

Jump to bottom

fix the maxfile_size checking bug #158

Closed DroidTest wants to merge 1 commit into jedisct1:master from DroidTest:master

Conversation 4 Commits 1 Checks 2 Files changed 1

DroidTest commented on Jul 29, 2021

Fix the predicate that never evaluates true.

Hi,

I occasionally found the PureFTPd continues to receive a file when user quota is exceeded. My debugging shows that the following predicates never evaluate true, since max_filesize =-1 initially:

(max_filesize >= (off_t) 0 &&
(max_filesize = user_quota_size - quota.size) < (off_t) 0)

When max_filesize >=(off_t) 0 evaluates false, the followed predicate will not be evaluated. Hence max_filesize =-1 for ever. This bug leads to that there is no overflow even if quota is exceeded.

For a simple patch, I changed the order of these two predicates such that max_filesize = user_quota_size - quota.size) < (off_t) 0 is evaluated first, then max_filesize will be assigned with the actual quota. Then quota will be checked correctly.

Bests
Joy

1

fix the maxfile_size checking bug ··· fb93975

ffontaine commented on Nov 22, 2021 Contributor

FYI, issue has been assigned CVE-2021-40524.

jedisct1 commented on Nov 23, 2021 Owner

Should be fixed in 37ad222 , thanks!

jedisct1 closed this on Nov 23, 2021

ffontaine commented on Nov 23, 2021 Contributor

Thanks for your prompt answer, I'll backport it on buildroot.
Do you plan a new release any time soon (latest one was made more than 2 years ago)?

ffontaine commented on Nov 23, 2021 Contributor

Thanks for this new release, I'll also bump our version of pure-ftpd in buildroot.

Reviewers
No reviews

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

3 participants