FreeNAS - Bug #34134

Fix corruption of first byte in AFP_AfpInfo stream/xattr in Samba

05/26/2018 08:23 AM - Andrew Walker

Status:	Done		
Priority:	No priority		
Assignee:	John Hixson		
Category:	OS		
Target version:	11.1-U6		
Seen in:	11.1-U4	**Needs Merging:**	No
Severity:	High	**Needs Automation:**	No
Reason for Closing:		**Support Suite Ticket:**	ZCX-891-77675
Reason for Blocked:	Other: make a note in comments	**Hardware Configuration:**	
Needs QA:	No	**ChangeLog Required:**	No
Needs Doc:	No		

Description

See also FreeBSD bug ticket here: https://bugs.freebsd.org/bugzilla/show_bug.cgi?id=228462

This has been observed on my own systems as well. Struct for AFP_AfpInfo is as follows:

```
typedef struct {
/*Ofs*/
/*  0*/    le32 signature;        /* Must be "AFP\0". */
/*  4*/    le32 version;        /* Must be 0x00010000. */
/*  8*/    le32 fileid;        /* This is the inode number as returned by the
                   AFP connection.  For some reason this is not
                   the same as the underlying NTFS inode
                   number.  Need to set this to zero on create,
                   preserve it on write, and ignore it on
                   read. */
/* 12*/    le32 backup_time;    /* Backup time for the file/dir in AppleDouble
                   time format (see above). */
/* 16*/    FINDER_INFO finder_info;/* Finder Info (32 bytes, see above). */
/* 48*/    PRODOS_INFO prodos_info;/* ProDOS Info (6 bytes, see above). */
/* 54*/ u8 reserved[6];        /* Reserved. */
/* sizeof() = 60 (0x3c) bytes */
```

AFP_AfpInfo prior to streams_xattr change is as follows:

```
root@cat_herder:/mnt/dozer/SOFIA_PHOTOS # getextattr -qq user 'DosStream.AFP_AfpInfo:$DATA' Finder
\ Refresh.app/ | hexdump -C
00000000  41 46 50 00 00 00 01 00  00 00 00 00 80 00 00 00  |AFP.............|
00000010  50 4c 41 50 6c 74 61 70  04 10 00 00 00 00 00 00  |PLAPltap........|
00000020  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00000030
```

After new streams_xattr:

```
00000000  00 46 50 00 00 00 01 00  00 00 00 00 00 00 00 80  |.FP.............|
00000010  50 4c 41 50 6c 74 61 70  04 10 00 00 00 00 00 00  |PLAPltap........|
00000020  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00000030
```

Ralph's explanation is as follows:
"vfs_streams_xattr to not read and write an additional trailing byte (cf the comment lines containing "// ? -1" in the patch), but when creating a stream the trailing byte is still stored (cf streams_xattr_open() the code after the comment "Darn, xattrs need at least 1 byte").

Due to a vicious interaction with a bug that is present in the latest macOS 10.13.4 (not sure about earlier versions) what happens is this:

- the client send a request to create a stream "file:AFP_AfpInfo"

- the server creates the xattr for the stream and writes a 0 byte

- the client sends a request to read 60 bytes at offset 0 from the stream

- the server returns a one byte sized buffer containing a 0 instead of returning nread=0 and status=NT_STATUS_END_OF_FILE

- the final nail in the coffin is that the client, when writing the AFP_AfpInfo blob whos first four byte start with a magic string "AFP" takes the 0 byte the server returned and overwrites the first byte of the magic string

The fix for this twofold: first, we must fix vfs_streams_xattr to not store an initial zero byte when creating an xattr. Second, we must prepare vfs_fruit to allow such broken AFP_AfpInfo blobs, otherwise users who adding vfs_fruit run into the issue that vfs_fruit has a builtin check for the magic string..."

Malformed signatures may cause undefined client behavior. We may be seeing this in the wild. Placing severity "high".

Related issues:

Related to FreeNAS - Bug #30702: Alternate Data Streams (ADS) with Fruit on S...	**Closed**
Copied to FreeNAS - Bug #36183: Fix corruption of first byte in AFP_AfpInfo s...	**Done**

Associated revisions

Revision e764a9dd - 06/18/2018 11:12 AM - Timur Bakeyev

Merge pull request #56 from freenas/FIX-34134-master

Fix 34134 master

Ticket: #34134

Revision edb6998e - 06/28/2018 08:56 AM - John Hixson

Restore original vfs_streams_xattr.c

Ticket: #34134

Revision ab7b2d99 - 06/28/2018 08:59 AM - John Hixson

Configurable buffer sizes for extended attributes

- This is a way simpler approach and is also based on what the Samba guys plan to do. This patch is based off of a patch by Ralph Boehme. It's known to work and keeps things simple. It also helps with keeping our tree in sync with Samba's tree.

- Minimum of 256 bytes

- Maximum of 16M
- Optimized for the 256 byte case, if larger, 16M is used

Ticket: #34134

Revision 24e97569 - 06/28/2018 11:17 AM - John Hixson

Standalone tool to fix AFP files with EA corruption

Ticket: #34134

Revision d9e4acff - 06/28/2018 11:22 AM - John Hixson

Bump samba port revision

Ticket: #34134

Revision 386bef03 - 07/03/2018 12:32 AM - John Hixson

Add ability to write out null byte at end of EA's

Ticket: #34134

Revision e3f98c0b - 07/03/2018 12:02 PM - John Hixson

Add ability to write out null byte at end of EA's (#1468)

- Add ability to write out null byte at end of EA's

Ticket: #34134

- Free stuff
- cosmetic stuff

Revision 024485c0 - 07/03/2018 01:29 PM - John Hixson

Reworked with recursive option, still a WIP

Ticket: #34134

Revision a5940b47 - 07/05/2018 12:19 PM - John Hixson

Standalone tool to fix AFP files with EA corruption

Ticket: #34134

Revision a88aa1ba - 07/05/2018 06:50 PM - John Hixson

Restore original vfs_streams_xattr.c

Ticket: #34134
(cherry picked from commit edb6998ee61a87f2e77b4b61b219d119afe0819f)

Revision 302a6eb1 - 07/05/2018 06:50 PM - John Hixson

Configurable buffer sizes for extended attributes

- This is a way simpler approach and is also based on what the Samba
guys plan to do. This patch is based off of a patch by Ralph Boehme.
It's known to work and keeps things simple. It also helps with keeping
our tree in sync with Samba's tree.

- Minimum of 256 bytes
- Maximum of 16M
- Optimized for the 256 byte case, if larger, 16M is used

Ticket: #34134
(cherry picked from commit ab7b2d99aa6e03efcaefd04f79835efdc7b73398)

Revision f8349a2c - 07/05/2018 06:54 PM - John Hixson

Bump Samba port revision

Ticket: #34134

Revision df0e3fd5 - 08/02/2018 11:47 PM - John Hixson

Configurable buffer sizes for extended attributes

- This is a way simpler approach and is also based on what the Samba
guys plan to do. This patch is based off of a patch by Ralph Boehme.
It's known to work and keeps things simple. It also helps with keeping
our tree in sync with Samba's tree.

- Minimum of 256 bytes
- Maximum of 16M
- Optimized for the 256 byte case, if larger, 16M is used

Ticket: #34134
(cherry picked from commit ab7b2d99aa6e03efcaefd04f79835efdc7b73398)

Revision b751f267 - 08/03/2018 11:06 AM - John Hixson

Standalone tool to fix AFP files with EA corruption

Ticket: #34134

(cherry picked from commit 24e97569c7f54f727e0b8d2b2710412079e7cd18)

Revision 3ed8061b - 08/03/2018 11:09 AM - John Hixson

Add ability to write out null byte at end of EA's (#1468)

- Add ability to write out null byte at end of EA's

Ticket: #34134

- Free stuff
- cosmetic stuff

(cherry picked from commit e3f98c0b678b1df027c35ad262929c090af3428f)

Revision db11b26d - 08/03/2018 11:10 AM - John Hixson

Standalone tool to fix AFP files with EA corruption

Ticket: #34134
(cherry picked from commit a5940b470952a600f1ef372046551b84b1cc17f8)

(11.1-stable)
Ticket: #34134

History

#1 - 05/26/2018 08:27 AM - Andrew Walker

- Assignee changed from Release Council to Timur Bakeyev

#2 - 05/26/2018 12:48 PM - Andrew Walker

- File new_streams_xattr.pcap added

- File old_streams_xattr.pcap added

#3 - 05/29/2018 05:43 AM - Sam Fourman

Master PR: https://github.com/freenas/samba/pull/55

#4 - 05/29/2018 05:50 AM - Dru Lavigne

- Status changed from Unscreened to In Progress

- Assignee changed from Timur Bakeyev to Andrew Walker

- Target version changed from Backlog to 11.2-RC2

#5 - 05/29/2018 05:56 AM - Sam Fourman

- Support Suite Ticket changed from n/a to ZCX-891-77675

#6 - 05/29/2018 06:13 AM - Andrew Walker

- Assignee changed from Andrew Walker to Timur Bakeyev

- Target version changed from 11.2-RC2 to 11.1-U5

#7 - 05/29/2018 06:55 AM - Dru Lavigne

- Target version changed from 11.1-U5 to 11.2-RC2

#12 - 05/29/2018 07:50 AM - Dru Lavigne

- File deleted (old_streams_xattr.pcap)

#13 - 05/29/2018 07:50 AM - Dru Lavigne

- File deleted (new_streams_xattr.pcap)

#14 - 05/29/2018 07:51 AM - Dru Lavigne

- Subject changed from vfs_streams_xattr triggers corruption of first byte in AFP_AfpInfo stream/xattr to Fix corruption of first byte in AFP_AfpInfo stream/xattr in Samba

- Status changed from In Progress to Ready for Testing

- Target version changed from 11.2-RC2 to 11.1-U6

- Needs Doc changed from Yes to No

- Needs Merging changed from Yes to No

#15 - 05/29/2018 07:51 AM - Dru Lavigne

- Private changed from Yes to No

#16 - 05/29/2018 11:17 AM - Dru Lavigne

- Status changed from Ready for Testing to In Progress

- Assignee changed from Timur Bakeyev to Andrew Walker

Andrew: we'll also need the stable PR to get this into testing.

#17 - 05/29/2018 04:29 PM - Dru Lavigne

- Assignee changed from Andrew Walker to Timur Bakeyev

As per discusion with Timur, more work needs to happen on this ticket.

#20 - 06/25/2018 09:13 AM - Ben Gadd

- Status changed from In Progress to Ready for Testing

#21 - 06/25/2018 12:14 PM - Dru Lavigne

Stable PR: https://github.com/freenas/samba/pull/57

#22 - 06/26/2018 11:15 AM - Ben Gadd

- Status changed from Ready for Testing to Blocked

- Reason for Blocked set to Other: make a note in comments

#24 - 06/27/2018 10:37 AM - Andrew Walker

- File new_streams_xattr.pcap added

- File old_streams_xattr.pcap added

#26 - 06/27/2018 12:35 PM - Andrew Walker

- File Finder Refresh.zip added

#30 - 06/28/2018 11:09 AM - Dru Lavigne

- Copied to Bug #36183: Fix corruption of first byte in AFP_AfpInfo stream/xattr in Samba added

#31 - 06/28/2018 11:15 AM - John Hixson

- Assignee changed from Timur Bakeyev to John Hixson

#32 - 06/28/2018 11:34 AM - John Hixson

I've proposed my solution to Timur & Mav. I'm waiting for Timur to respond. I think we need to restore vfs_streams_xattr.c to the original version that Samba uses. The re-work of the module is overly complicated and has many problems with it not even counting the corruption that is occurring. We can make large extended attributes configurable in a much easier way that is compatible with how Samba plans to do them. I've added this to the pull request. I've also written a standalone tool to fix files that were corrupted.

Samba master PR: https://github.com/freenas/samba/pull/59
FreeNAS master PR: https://github.com/freenas/freenas/pull/1455

#33 - 06/28/2018 11:53 AM - John Hixson

- Status changed from Blocked to Ready for Testing

#34 - 06/28/2018 02:55 PM - John Hixson

- Status changed from Ready for Testing to In Progress

#39 - 07/05/2018 12:30 PM - Joe Maloney

https://github.com/freenas/freenas/pull/1480

#40 - 07/05/2018 12:33 PM - Joe Maloney

https://github.com/freenas/freenas/pull/1481

#41 - 07/05/2018 03:02 PM - Timur Bakeyev

I think there is a mix up between #34134 and #36183. First one is for 11.1-U6 and the second one is for 11.2b1.

My understanding is that John provided his fix for 11.2b1 in #36183, while this ticket is for the 11.1-U6 and the fix for it should be

https://github.com/freenas/samba/pull/57

In general I wouldn't do any radical changes in an upgrade between U5 to U6. But correct me, if I'm wrong.

#42 - 07/05/2018 06:03 PM - John Hixson

Timur Bakeyev wrote:

> I think there is a mix up between #34134 and #36183. First one is for 11.1-U6 and the second one is for 11.2b1.
>
> My understanding is that John provided his fix for 11.2b1 in #36183, while this ticket is for the 11.1-U6 and the fix for it should be
>
> https://github.com/freenas/samba/pull/57
>
> In general I wouldn't do any radical changes in an upgrade between U5 to U6. But correct me, if I'm wrong.

There is no mix up here. The same fix for 11.2b1 will be going out in 11.1-U6.

#43 - 07/05/2018 06:17 PM - John Hixson

So there isn't really a problem here. Large EA's work fine. The only "problem" that happens is when a file with a large EA over what is a predefined size is copied to the local file system, it gets truncated. This isn't the general use case and this has worked this way all along. I don't even think this can be classified as a bug. I think we are good to go here and there are no more show stoppers.

#44 - 07/09/2018 09:36 AM - Dru Lavigne

- Status changed from In Progress to Ready for Testing

#45 - 07/18/2018 03:55 PM - Timur Bakeyev

- Related to Bug #30702: Alternate Data Streams (ADS) with Fruit on SMB share problem added

#46 - 08/02/2018 11:31 AM - Dru Lavigne

11.1-stable PR: https://github.com/freenas/samba/pull/60

#47 - 08/03/2018 01:21 PM - John Hixson

11.1-stable PR: https://github.com/freenas/freenas/pull/1631

#48 - 08/05/2018 11:10 AM - Dru Lavigne

- Status changed from Ready for Testing to In Progress

- Needs Merging changed from No to Yes

#49 - 08/06/2018 02:14 PM - Dru Lavigne

- Status changed from In Progress to Ready for Testing

- Needs Merging changed from Yes to No

#50 - 08/15/2018 11:36 AM - Bonnie Follweiler

- Status changed from Ready for Testing to Passed Testing

- Needs QA changed from Yes to No

Passed testing in FreeNAS 11.1-U6 Internal4

#51 - 08/15/2018 01:35 PM - Dru Lavigne

- Status changed from Passed Testing to Done

Files

old_streams_xattr.pcap	1.21 MB	06/27/2018	Andrew Walker
new_streams_xattr.pcap	1.47 MB	06/27/2018	Andrew Walker
Finder Refresh.zip	74.3 KB	06/27/2018	Andrew Walker