Tails - Bug #15829

Harden sudo config to avoid potential future privilege escalation

08/21/2018 02:24 PM - intrigeri

<table>
<thead>
<tr>
<th>Status:</th>
<th>Resolved</th>
<th>Start date:</th>
<th>08/21/2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
<td>Due date:</td>
<td></td>
</tr>
<tr>
<td>Assignee:</td>
<td></td>
<td>% Done:</td>
<td>100%</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
<td>Estimated time:</td>
<td>1.00 hour</td>
</tr>
<tr>
<td>Target version:</td>
<td>Tails_3.10.1</td>
<td>Spent time:</td>
<td>0.00 hour</td>
</tr>
<tr>
<td>Feature Branch:</td>
<td>bugfix/15829-harden-sudo-config+force-all-tests</td>
<td>Starter:</td>
<td></td>
</tr>
<tr>
<td>Type of work:</td>
<td>Code</td>
<td>Estimated time:</td>
<td>1.00 hour</td>
</tr>
<tr>
<td>Blueprint:</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Description

blocks Tails - Feature #15506: Core work 2018Q4: Foundations Team
Resolved 04/08/2018

Related issues:

- Blocks Tails - Feature #15506: Core work 2018Q4: Foundations Team

Associated revisions

Revision 55473230 - 08/22/2018 11:59 AM - intrigeri

Harden sudo configuration (refs: #15829).

This should not be needed because at the moment, none of these commands do anything with their command-line arguments (except poweroff and reboot but their argument don't allow further privilege escalation), but better safe than sorry.

Revision 9554ae27 - 10/20/2018 10:15 AM - intrigeri

Merge branch `bugfix/15829-harden-sudo-config+force-all-tests` into stable (Fix-committed: #15829)

History

#2 - 08/21/2018 02:25 PM - intrigeri
- Blocks Feature #15334: Core work 2018Q3: Foundations Team added

#3 - 08/22/2018 11:53 AM - intrigeri
- Subject changed from Review sudo config for potential privilege escalation to Harden sudo config to avoid potential future privilege escalation
- Description updated
- Status changed from Confirmed to In Progress
- Priority changed from High to Normal
- Target version changed from Tails_3.9 to Tails_3.10.1
- % Done changed from 0 to 10
- Private changed from Yes to No
- Feature Branch set to bugfix/15829-harden-sudo-config+force-all-tests
- Type of work changed from Security Audit to Code

#4 - 08/22/2018 04:24 PM - intrigeri
- Assignee changed from intrigeri to segfault
- Estimated time set to 1.00 h
1h because it would be nice to manually test the affected bits that our automated test suite does not exercise (i.e. I think only the boot profile part).

#5 - 08/22/2018 04:25 PM - intrigeri  
- % Done changed from 10 to 50

Forgot to say: it passes our full automated test suite.

#6 - 10/08/2018 01:59 PM - intrigeri  
- Blocks deleted (Feature #15334: Core work 2018Q3: Foundations Team)

#7 - 10/08/2018 01:59 PM - intrigeri  
- Blocks Feature #15506: Core work 2018Q4: Foundations Team added

#8 - 10/12/2018 02:04 PM - intrigeri  
- Assignee changed from segfault to lamby

(I think segfault has plenty enough on his plate for 3.10 => reassigning.)

@lamby: see comments above wrt. what should be manually tested. Thanks!

#9 - 10/18/2018 09:53 PM - lamby

For those following along at home:

you can [append] ** to indicate that the command may only be run without command line arguments

#10 - 10/19/2018 09:12 PM - lamby  
- File 2018-10-19_17-07.png added  
- Assignee changed from lamby to intrigeri  
- QA Check changed from Ready for QA to Pass

Methodology:

I built branch bugfix/15829-harden-sudo-config+force-all-tests at a42340eb8ae681ed279826e3f11191f8c5869a26 to generate tails-amd64-bugfix_15829-harden-sudo-config+force-all-tests-3.10-20181019T1930Z-a42340eb8a.iso which has a SHA1 of c88ebd186e373d23874fc4a09304233f836644.

Expected behaviour:

/usr/local/sbin/tails-debugging-info (and friends) should reject any parameters when run under sudo. Running without parameters should work as before/expected.

Saw behaviour:

$ sudo /usr/local/sbin/tails-debugging-info DISALLOW was rejected. $ sudo /usr/local/sbin/tails-debugging-info was allowed. See attached screenshot.

Conclusion:

I consider this tested, working and ready to merge.
#11 - 10/20/2018 08:56 AM - intrigeri

Thank you. I'll test the "boot profile" part myself (mentioned in #15829#note-4 but clearly lacking pointers for you to understand what I was talking about; FTR this is about the code we have for "SquashFS file order" in https://tails.boum.org/contribute/release_process/) because it's probably too late to do another round-trip in time for 3.10. If that works, I'll merge.

#12 - 10/20/2018 08:58 AM - intrigeri

lamby wrote:

Expected behaviour:

/usr/local/sbin/tails-debugging-info (and friends) should reject any parameters when run under sudo. Running without parameters should work as before/expected.

FTR the sudo config for tails-debugging-info was hardened 3.5 years ago and is not affected by the proposed branch.

#13 - 10/20/2018 09:03 AM - intrigeri

- QA Check changed from Pass to Ready for QA

#14 - 10/20/2018 10:16 AM - intrigeri

- Status changed from In Progress to 11
- Assignee deleted (intrigeri)
- % Done changed from 50 to 100
- QA Check changed from Ready for QA to Pass

intrigeri wrote:

Thank you. I'll test the "boot profile" part myself (mentioned in #15829#note-4 but clearly lacking pointers for you to understand what I was talking about; FTR this is about the code we have for "SquashFS file order" in https://tails.boum.org/contribute/release_process/)

That works: the boot-profile process is correctly killed.

If that works, I'll merge.

Done! :)

05/15/2020
If it helps, I also tested poweroff but naturally could not get a screenshot of it so thus did not use it as my documented testcase.

- Status changed from 11 to In Progress

Applied in changeset commit:d9c6ac1a2b83e62808921bd0f5ea88dd9bd343aa.

- Status changed from In Progress to Resolved

Files

<table>
<thead>
<tr>
<th>Filename</th>
<th>Size</th>
<th>Date</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018-10-19_17-07.png</td>
<td>78.2 KB</td>
<td>10/19/2018</td>
<td>lamby</td>
</tr>
</tbody>
</table>