openQA Tests - action #93886

[sle][security][sle15sp4]automate testing of scap-security-guide

2021-06-11 09:42 - msmeissn

Status:	New	**Start date:**	2021-06-11
Priority:	Normal	**Due date:**	
Assignee:	llzhao	**% Done:**	0%
Category:	New test	**Estimated time:**	0.00 hour
Target version:			
Difficulty:			

Description

we now have a "stig" hardening in the scap-security-guide

can you add testing for this to SLES, for both:

- detection mode
- mitigation mode

and also test if regular SLES stuff continues to work after running mitigation.
(e.,g. having a installation flavor regular + stig hardening mitigation)

History

#1 - 2021-06-21 07:44 - maritawerner

- Subject changed from automate testing of scap-security-guide to [security]automate testing of scap-security-guide

#2 - 2021-07-01 08:40 - llzhao

- Subject changed from [security]automate testing of scap-security-guide to [sle][security][sle15sp4]automate testing of scap-security-guide

- Category set to New test

- Assignee set to llzhao

#3 - 2021-07-01 08:50 - llzhao

msmeissn wrote:

> we now have a "stig" hardening in the scap-security-guide
>
> can you add testing for this to SLES, for both:
>
> - detection mode
> - mitigation mode
>
> and also test if regular SLES stuff continues to work after running mitigation.
> (e.,g. having a installation flavor regular + stig hardening mitigation)

msmeissn , could please offer more info (any docs/links) on the "scap-security-guide"?
We do not have any idea atm. Thanks!

#4 - 2021-07-05 06:48 - llzhao

After investigation found these helpful links:

1. confluence page: https://confluence.suse.com/display/SecurityCertifications/Hardening+workshop+preparation
https://confluence.suse.com/display/GEHC/General+Security+Discussions
2. JIRA feature: https://jira.suse.com/browse/PM-2390https://jira.suse.com/browse/PM-245
3. sles15sp3 GM # zypper se -s scap-security-guide

S	Name	Type	Version	Arch	Repository
	scap-security-guide	package	0.1.55git20210323-1.10.1	noarch	SLE-Module-Basesystem15-SP3-Pool

...

1. man page of scap-security-guide ... Profiles in Guide to the Secure Configuration of SUSE Linux Enterprise 15 ... Additional details can be found on the projects wiki page: https://www.github.com/OpenSCAP/scap-security-guide/wiki ...

#5 - 2021-07-06 14:40 - msmeissn

ok, simple approaches:

install openscap-utils

on SLE15 all servicepacks: (just replace sle15 by sle12 in SLE12)
oscap xccdf eval --profile stig /usr/share/xml/scap/ssg/content/ssg-sle15-ds.xml

this is the basic evaluation and will print to stdout. There are some output optipons too which could be used for easier scripting if needed.

There is a mitigation mode:
oscap xccdf remediate --profile stig /usr/share/xml/scap/ssg/content/ssg-sle15-ds.xml

DANGER NOTE: this WILL change your system and might disallow logins or similar, so only use in scratch vms for testing or when you are able to recover it.

You can take a look at the existing openscap tests in openqa too and inject the ssg-sle15-ds.xml or ssg-sle12-ds.xml there

#6 - 2021-07-09 00:39 - llzhao

Got it, thanks for the info.