SUSE Linux Enterprise Server

Hardening SUSE Linux Enterprise with OpenSCAP

This document introduces you to auditing and hardening SUSE Linux Enterprise with OpenSCAP and the `SCAP Security Guide`.

Publication Date: September 29, 2024

Contents

Important: Disclaimer

SUSE seeks to provide customers with quick and easy guides that can assist them in maintaining security compliance. Implementation of the settings contained within this guide without its prior testing in a non-operational environment is highly discouraged. The developers of these profiles and documentation have made reasonable efforts to ensure overall compliance. They assume no responsibility for its use by other parties, and make no guarantee, expressed or implied, about its quality, reliability or any other characteristic.

1 What are SCAP and OpenSCAP?

SCAP stands for `Security Content Automation Protocol`. It is a framework of specifications that support automated configuration, vulnerability scanning, and policy compliance evaluation of systems deployed in an organization. It also standardizes how vulnerabilities and security configurations are communicated both to machines and human beings.

OpenSCAP is a collection of open source tools that implement the SCAP framework for Linux. SCAP is maintained by the National Institute of Standards and Technology (NIST) . OpenSCAP received the SCAP 1.2 certification by NIST in 2014.

2 Benefits

The OpenSCAP tools, together with the `SCAP Security Guide`, can be used for auditing your system in an automated way. The `SCAP Security Guide` implements security guidances recommended by respected authorities. These security guidances are transformed into a machine-readable format which then can be used by OpenSCAP and other tools.

3 Installation

To use the OpenSCAP tools and the `SCAP Security Guide` for hardening your target system by scanning and remediating vulnerabilities, install the following core packages:

- `openscap`
- `openscap-utils`
- `scap-security-guide`

```
> sudo zypper install openscap openscap-utils scap-security-guide
```

Note

These packages are dependencies for other optional packages discussed below.

Optionally, install the following packages:

- `scap-workbench`: This package provides the SCAP Workbench graphical utility to perform common `oscap` tasks.
- `ssg-apply`: When used along with SCAP Workbench, this package helps you conveniently apply a tailoring file for customized hardening.

```
> sudo zypper install scap-workbench scap-workbench-doc ssg-apply
```

Tip: Security best practice for SCAP Workbench

As a security best practice, avoid installing an application software such as SCAP Workbench on the target system that you are planning to harden. Instead, install SCAP Workbench on a client machine and apply the hardening on the target system, while maintaining an air gap before the target system is connected to a potentially insecure network.

4 Important SCAP components

SCAP consists of the following important components which interact with each other.

Open Vulnerability and Assessment Language (OVAL)

An XML format for testing the presence of a specific state.

Extensible Configuration Checklist Description Format (XCCDF)

An XML format that specifies security checklists, benchmarks and configuration documentation. The XCCDF file includes a benchmark as a set of different profiles related to different groups. Each group is a set of rules which have OVAL definitions. Each profile is related to different good practices such as STIG, HIPAA, PCI-DSS, or ANSSI.

Common Platform Enumeration (CPE)

A structured naming scheme to identify information technology systems, platforms and software packages. It is maintained by NIST and NDV. The naming scheme consists of the following elements: `cpe:/part:vendor:product:version:update:edition:language`

DataStreams (DS)

An XML format which packs different SCAP components (CPE, XCCDF, OVAL) into a single file. It can be used to distribute SCAP content over the network. The DataStreams files are useful because they include everything you need when you want to harden and audit your SUSE Linux Enterprise system.

Common Configuration Enumeration (CCE)

Unique identifiers to security-related system configuration issues.

5 SCAP Security Guide content and directories

SUSE ships the `SCAP Security Guide` (SSG) toolset in the `scap-security-guide` package. It contains the latest set of security polices for Linux systems. The `SCAP Security Guide` is maintained upstream in the ComplianceAsCode (https://github.com/ComplianceAsCode/) repository.

After you have installed the package, the SSG security content and the related files are available in your system from the following directories:

OVERVIEW OF FILES AND DIRECTORIES

`/usr/share/xml/scap/ssg/content/`

Contains the SSG security content. It consists of several *Important SCAP components*, which are all based on XML. All XML files in that directory are named according to the SCAP component and to the SUSE Linux Enterprise codestream they apply to (code 12 or 15). The directory also holds XML files specific to openSUSE.

`/usr/share/doc/scap-security-guide/guides/`

Contains profiles for different hardening policies in human-readable format. They describe the profiles that are included in the DataStream files. The profiles applicable to SUSE Linux Enterprise are codestream-specific and differ between code 12 and code 15. Each profile is a guide on securing your operating system to ensure compliance with a regulation.
The guides usually have the following structure:

- Short description
- Profile Title. For example: *DISA STIG for SUSE Linux Enterprise 15*
- Profile ID. For example: *xccdf_org.ssgproject.content_profile_stig*
- Revision History. Information about the current version and status of the profile. For example: *xccdf_org.ssgproject.content_profile_stig*
- Platforms (in CPE notation). Which product or system the profile applies to. For example: *cpe:/o:suse:linux_enterprise_server:15*
- A table of contents
- A checklist which consists of groups (and subgroups) with rules
  Each rule consists of a short description, the rationale behind the rule, a severity (low, medium or high) and a unique identifier in the `Common Configuration Enumeration (CCE)` format. The CCE number for each rule is provided to SUSE by NIST. Each rule also lists references to different good practices. For example, the rule known by the unique identifier `CCE-83289-9` in STIG has a reference to a specific good practice `A.12.4.1` in ISO/IEC 27001:2013.
  If remediation options exist for a rule, they are listed in different formats.

`/usr/share/scap-security-guide`

Contains subdirectories with fix scripts which can be used to remediate the target system in case a vulnerability is found during a scan. Fix scripts are available in the following two formats: Shell scripts (`bash/*.sh`) and Ansible snippets (`ansible/*.yml`).

6 SCAP Security Guide profiles

The `SCAP Security Guide` contains multiple profiles. The profiles applicable to SUSE Linux Enterprise are codestream-specific and differ between code 12 and code 15.

They are maintained and hosted at the following repositories:

- https://github.com/ComplianceAsCode/content/tree/master/products/sle15/profiles
- https://github.com/ComplianceAsCode/content/tree/master/products/sle12/profiles

After the installation of the `scap-security-guide` package, human-readable versions of the profiles are available in your file system in `/usr/share/doc/scap-security-guide/guides`. Alternatively, find the same content online as static HTML pages:

- https://static.open-scap.org/ssg-guides/ssg-sle15-guide-index.html
- https://static.open-scap.org/ssg-guides/ssg-sle12-guide-index.html

In the online versions, use the drop-down list in the upper-right corner of the page to select one of the available profiles and to view a command-line snippet about how to evaluate the respective profile with OpenSCAP.

6.1 SUSE Linux Enterprise 15 profiles

For code 15, the following profiles are supported by SUSE:

- ANSSI-BP-028 (enhanced)
- ANSSI-BP-028 (high)
- ANSSI-BP-028 (intermediary)
- ANSSI-BP-028 (minimal)
- CIS SUSE SUSE Linux Enterprise 15 Benchmark Level 2 (Workstation)
- CIS SUSE Linux Enterprise 15 Benchmark for Level 1 (Server)
- CIS SUSE Linux Enterprise 15 Benchmark for Level 1 (Workstation)
- CIS SUSE Linux Enterprise 15 Benchmark for Level 2 (Server)
- DISA STIG for SUSE Linux Enterprise 15
- Hardening for Public Cloud Image of SUSE Linux Enterprise Server (SLES) for SAP Applications 15
- Health Insurance Portability and Accountability Act (HIPAA)

- PCI-DSS v4 Control Baseline for SUSE Linux Enterprise 15
- Public Cloud Hardening for SUSE Linux Enterprise 15
- Standard System Security Profile for SUSE Linux Enterprise 15

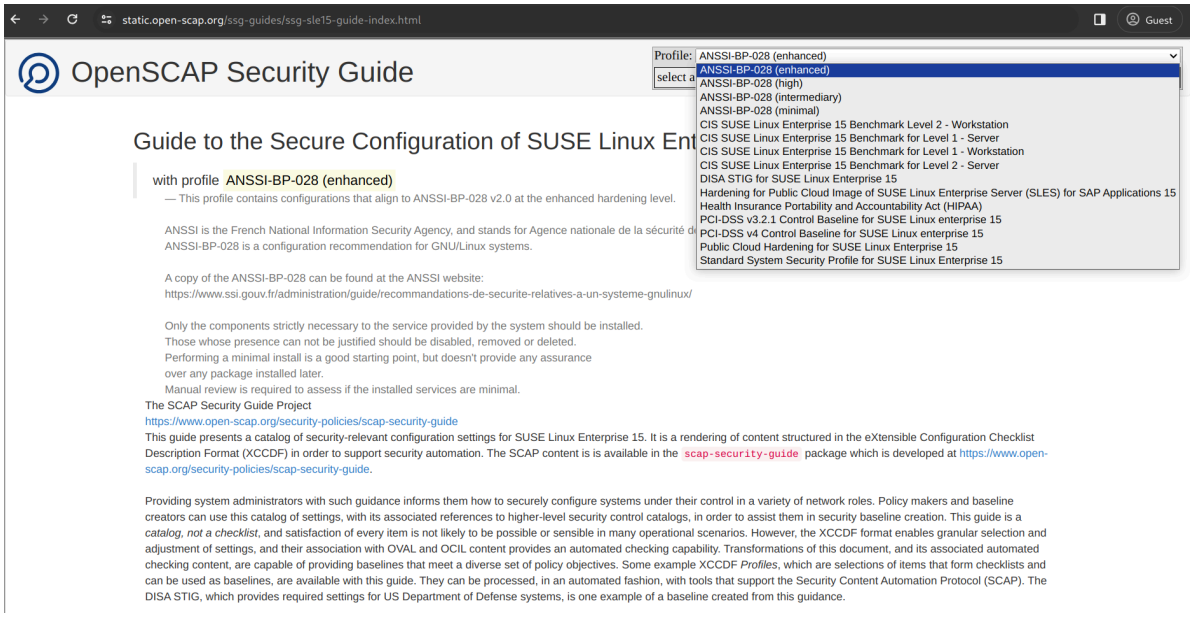

FIGURE 1: SCAP SECURITY GUIDE PROFILES FOR SUSE LINUX ENTERPRISE 15

6.2 SUSE Linux Enterprise 12 profiles

For code 12, the following profiles are supported by SUSE:

- ANSSI-BP-028 (enhanced)
- ANSSI-BP-028 (high)
- ANSSI-BP-028 (intermediary)
- ANSSI-BP-028 (minimal)
- CIS SUSE SUSE Linux Enterprise 12 Benchmark Level 2 (Workstation)
- CIS SUSE Linux Enterprise 12 Benchmark for Level 1 (Server)
- CIS SUSE Linux Enterprise 12 Benchmark for Level 1 (Workstation)
- CIS SUSE Linux Enterprise 12 Benchmark for Level 2 (Server)

- DISA STIG for SUSE Linux Enterprise 12
- PCI-DSS v.4 Control Baseline for SUSE Linux Enterprise 12
- Standard System Security Profile for SUSE Linux Enterprise 12

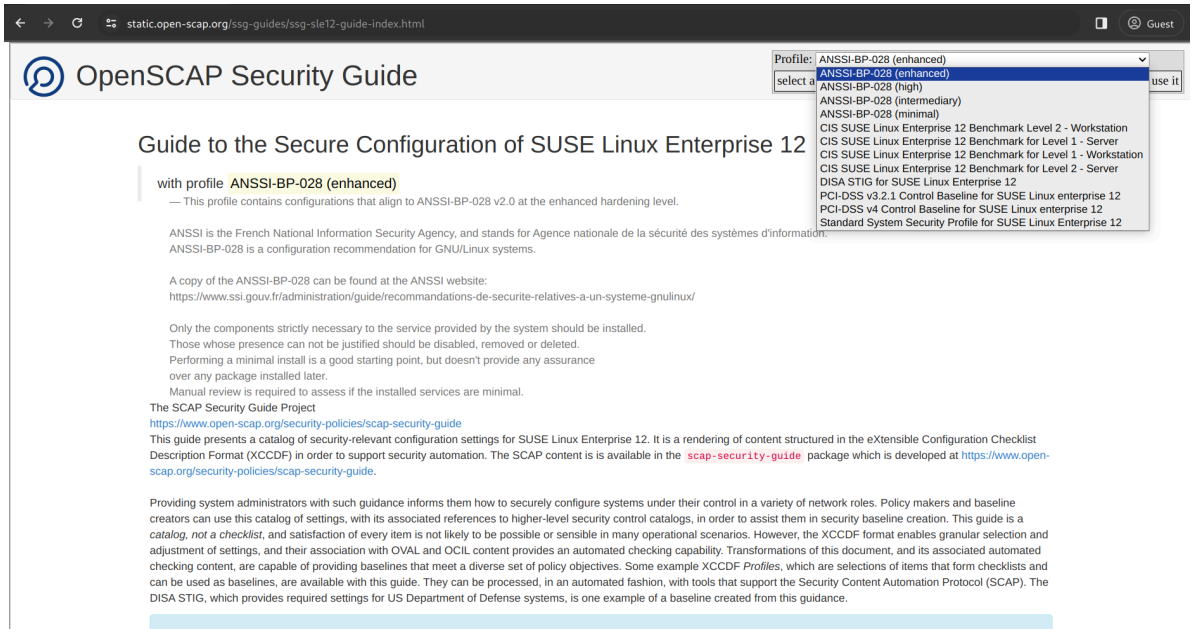

FIGURE 2: SCAP SECURITY GUIDE PROFILES FOR SUSE LINUX ENTERPRISE 12

7 Vulnerability scanning

7.1 Targets to scan

The content provided by the `SCAP Security Guide` can be used to scan the following targets for vulnerabilities:

- bare-metal machines
- virtual machines
- virtual machine images
- containers
- container images

Automated checks help to identify the target and to select only the rules that make sense for this specific target. For example, checks for separate partitions make sense for bare-metal machines but not for containers.

7.2 Tools for scanning

Note

Before using the tools described in this section, ensure that you have installed them as described in *Section 3, "Installation"*, as they are interdependent.

Depending on your setup and the target to scan (remote or local), you can use either of the following tools:

oscap

A command-line interface that can be used to scan local machines. Both the `openscap-utils` and `scap-security-guide` package need to be installed on the local machine.

To understand the basic usage of **`oscap`**, run it with the **`-h`** option:

```
> oscap -h

  oscap

  OpenSCAP command-line tool

  Usage: oscap [options] module operation [operation-options-and-arguments]

  Common options:
    --verbose <verbosity_level>   - Turn on verbose mode at specified verbosity
level.
                                    Verbosity level must be one of: DEVEL, INFO,
WARNING, ERROR.
    --verbose-log-file <file>     - Write verbose information into file.

  oscap options:
    -h --help                     - show this help
    -q --quiet                    - quiet mode
    -V --version                  - print info about supported SCAP versions

  Commands:
```

```
      ds - Data stream utilities
      oval - Open Vulnerability and Assessment Language
      xccdf - eXtensible Configuration Checklist Description Format
      cvss - Common Vulnerability Scoring System
      cpe - Common Platform Enumeration
      cve - Common Vulnerabilities and Exposures
      cvrf - Common Vulnerability Reporting Framework
      info - Print information about a SCAP file.
```

To understand `oscap` in greater detail, read its man pages by running the **`man oscap`**.

oscap-ssh

A command-line interface that can be used to scan a remote machine via SSH with an interface resembling the **`oscap`** tool. On the local machine, the package `openscap-utils` needs to be installed. On the remote machine, the `openscap-utils` package needs to be installed.

To understand the basic usage of **`oscap-ssh`**, run it with the **`-h`** option:

```
> oscap -h

  oscap-ssh -- Tool for running oscap over SSH and collecting results.

  Usage:

  $ oscap-ssh user@host 22 info INPUT_CONTENT
  $ oscap-ssh user@host 22 xccdf eval [options] INPUT_CONTENT

  Only source data streams are supported as INPUT_CONTENT!

  supported oscap xccdf eval options are:
    --profile
    --tailoring-file
    --tailoring-id
    --cpe (external OVAL dependencies are not supported yet!)
    --oval-results
    --results
    --results-arf
    --report
    --skip-valid
    --skip-validation
    --fetch-remote-resources
    --local-files
    --progress
    --datastream-id
    --xccdf-id
    --benchmark-id
```

```
    --remediate

  $ oscap-ssh user@host 22 oval eval [options] INPUT_CONTENT

  supported oscap oval eval options are:
    --id
    --variables
    --directives
    --results
    --report
    --skip-valid
    --skip-validation
    --datastream-id
    --oval-id

  $ oscap-ssh user@host 22 oval collect [options] INPUT_CONTENT

  supported oscap oval collect options are:
    --id
    --syschar
    --variables
    --skip-valid
    --skip-validation

  specific option for oscap-ssh (must be first argument):
    --sudo

  To supply additional options to ssh/scp, define the SSH_ADDITIONAL_OPTIONS
variable
  For instance, to ignore known hosts records, define SSH_ADDITIONAL_OPTIONS='-o
StrictHostKeyChecking=no -o UserKnownHostsFile=/dev/null'

  specific option for oscap-ssh (must be first argument):

  See `man oscap` to learn more about semantics of these options.
```

To understand `oscap-ssh` in greater detail, read its man pages by running **`man oscap-ssh`**.

SCAP Workbench

SCAP Workbench is a graphical user interface for OpenSCAP. You can use it for convenience instead of using `oscap`. For example, you can use SCAP Workbench for scanning a single machine, either local or remote (via SSH).

To use SCAP Workbench, both the `scap-workbench` and `scap-security-guide` packages need to be installed on the local machine. On the remote machine, the `openscap-utils` package needs to be installed.

To start SCAP Workbench, run the following command:

```
> scap-workbench
```

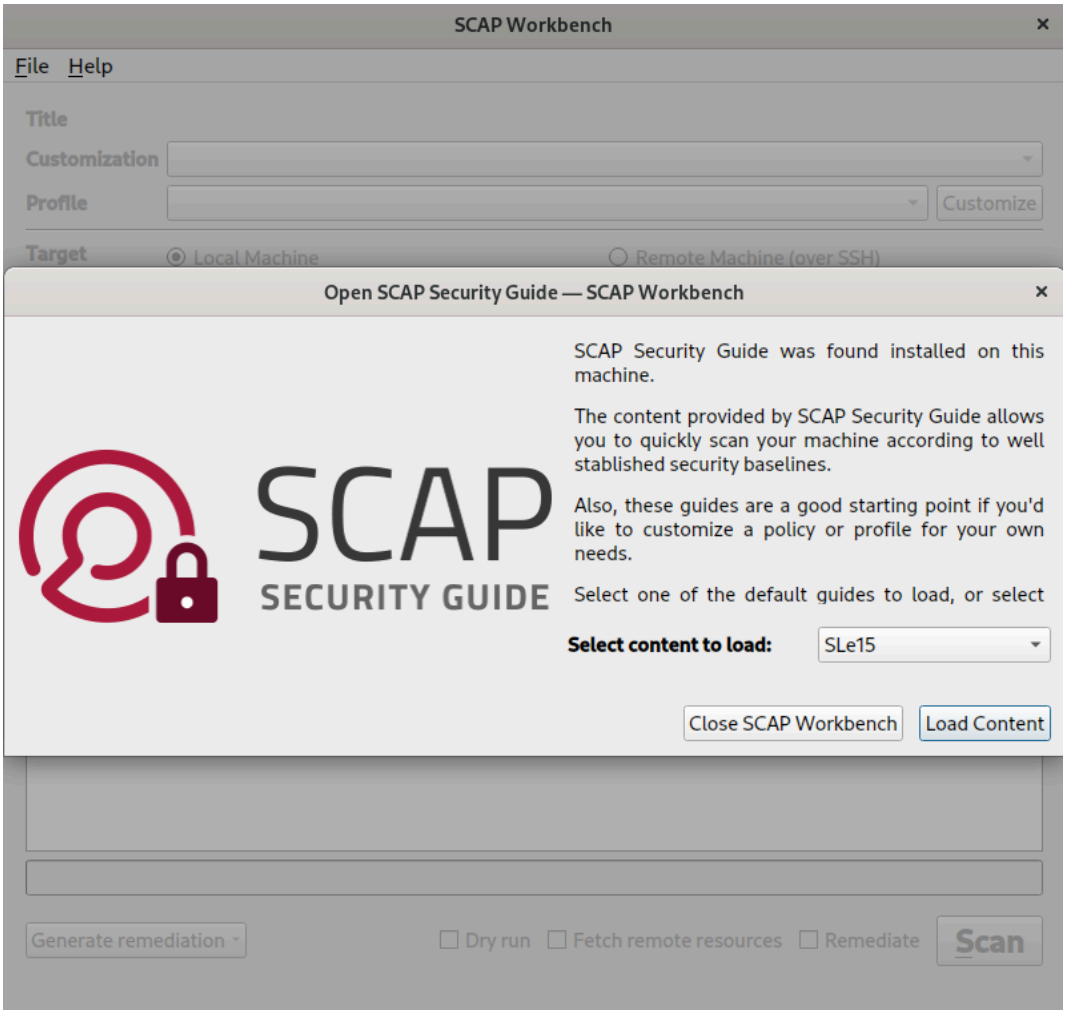

FIGURE 3: SCAP WORKBENCH

Although not recommended, you can invoke and perform certain basic operations by using SCAP Workbench as a command-line tool. To know more, read its man page by running `man scap-workbench`.

7.3 Scanning a SUSE Linux Enterprise system

The following example shows how to scan SUSE Linux Enterprise 15 locally with `oscap` for vulnerability issues according to a certain profile. You can save the results in XML format and generate an HTML report.

EXAMPLE 1: SCANNING SUSE LINUX ENTERPRISE WITH OSCAP

```
> sudo oscap xccdf eval❶ \
    --profile stig❷ \
    --results /tmp/results.xml❸ \
    --report /tmp/report.html❹ \
    /usr/share/xml/scap/ssg/content/ssg-sle15-ds.xml❺
```

❶ Calls the **`oscap xccdf`** module and tells it to perform an evaluation (vulnerability scan).

❷ Specifies the profile to use, in this case, `stig`.

❸ Saves the results of the evaluation to */tmp/results.xml*.

❹ Generates an HTML report called */tmp/report.html* in addition to the results in XML.

❺ Specifies the `SCAP Security Guide` policy file to use. In this example, we use a policy file in the `DataStream` format that applies to SUSE Linux Enterprise code 15. To list all available policies, run: **`ls -1 /usr/share/xml/scap/ssg/content/ssg-*-ds.xml`**. For more information about a particular policy, run **`oscap info`** on the file.

The evaluation process usually takes a few minutes, depending on the number of selected rules.

7.4 Using external or remote resources for scanning

SCAP content may reference external resources. For example, the SCAP Security Guide uses an external OVAL file to check whether the system is up to date and patched against known security vulnerabilities. However, OpenSCAP can handle remote resources differently, based on the options used while invoking the **`oscap`** command. In addition, you can use strategies like downloading specific remote resources in advance, and pointing the OpenSCAP tool towards the downloaded resources while invoking it.

7.4.1 Default warning for remote resources by OpenSCAP while performing evaluation

While evaluating SCAP content with external resources, the OpenSCAP tool displays a **warning**. For example, OpenSCAP displays the following warning while performing the default evaluation of a system based on the SCAP Security Guide:

```
> sudo oscap xccdf eval \
--profile xccdf_org.ssgproject.content_profile_stig \
--results ssg-sle15-xccdf-stig-results.xml \
/usr/share/xml/scap/ssg/content/ssg-sle15-ds.xml

WARNING: Datastream component 'scap_org.open-scap_cref_pub-projects-security-oval-
suse.linux.enterprise.15-
patch.xml.bz2' points out to the remote 'https://ftp.suse.com/pub/projects/security/oval/
suse.linux.enterprise.
15-patch.xml.bz2'. Use '--fetch-remote-resources' option to download it.

WARNING: Skipping 'https://ftp.suse.com/pub/projects/security/oval/
suse.linux.enterprise.15-patch.xml.bz2' file
which is referenced from datastream

WARNING: Skipping ./pub-projects-security-oval-suse.linux.enterprise.15-patch.xml.bz2
 file which is referenced
from XCCDF content
```

The following sections describe certain strategies to force OpenSCAP to fetch remote resources in real time, or download them in advance and use for evaluation and scanning the system.

7.4.2 Fetching remote resources for evaluation

If you trust your local content and the remote content it references, you can use the `--fetch-remote-resources` option to automatically download it when invoking the OpenSCAP tool.

```
> sudo oscap xccdf eval \
--fetch-remote-resources \
--profile xccdf_org.ssgproject.content_profile_stig \
--results ssg-sle15-xccdf-stig-results.xml \
/usr/share/xml/scap/ssg/content/ssg-sle15-ds.xml

Downloading: https://ftp.suse.com/pub/projects/security/oval/suse.linux.enterprise.15-
patch.xml.bz2 ... ok

--- Starting Evaluation —
```

```
...
```

However, if access to the Internet is unavailable at the time of evaluation, or is considered a security risk, you can instruct OpenSCAP to use local files instead of remote resources.

7.4.3 Downloading and saving remote resources locally for evaluation

On systems without Internet access, or in security sensitive deployments where OpenSCAP cannot connect to the Internet, download the remote content using other tools and save it locally. You can then pass it to OpenSCAP as a local file using the `--local-files` option, instead of the `--fetch-remote-resources` option.

For example, to prevent OpenSCAP from accessing the Internet but still use the patch file https://ftp.suse.com/pub/projects/security/oval/suse.linux.enterprise.15-patch.xml.bz2, perform the following procedure.

1. *(Optional)* Create a directory for storing the downloaded remote resources.

```
> mkdir ~/scap-files (1)
```

(1) Directory to store downloaded remote resources. If you have identified a suitable directory, skip this step.

2. Download the remote resource and save it as a local file.

```
> wget -O ~/scap-files/pub-projects-security-oval-suse.linux.enterprise.15-
patch.xml.bz2(1) \
https://ftp.suse.com/pub/projects/security/oval/suse.linux.enterprise.15-
patch.xml.bz2(2)
```

(1) The path to the locally saved file.

(2) The remote resource to be downloaded and saved locally.

Note

In this example, the name of the local file is **not** arbitrary. Notice the following information in the SCAP source data stream file available at `/usr/share/xml/scap/ssg/content/ssg-sle15-ds.xml`:

```
> cat /usr/share/xml/scap/ssg/content/ssg-sle15-ds.xml | \
grep -n "scap_org.open-scap_cref_pub-projects-security-oval-
suse.linux.enterprise.15-patch.xml.bz2"
```

```
17:          <cat:uri name="pub-projects-security-oval-
suse.linux.enterprise.15.xml" uri="#scap_org.open-scap_cref_pub-projects-
security-oval-suse.linux.enterprise.15-patch.xml.bz2"/>
25:      <ds:component-ref id="scap_org.open-scap_cref_pub-projects-
security-oval-suse.linux.enterprise.15-patch.xml.bz2" xlink:href="https://
ftp.suse.com/pub/projects/security/oval/suse.linux.enterprise.15-
patch.xml.bz2"/>
```

3. Run the evaluation using the local files downloaded earlier from the remote source.

```
> sudo oscap xccdf eval \
 --local-files ~/scap-files \
 --profile xccdf_org.ssgproject.content_profile_stig \
 --results ssg-sle15-xccdf-stig-results.xml \
 /usr/share/xml/scap/ssg/content/ssg-sle15-ds.xml

 WARNING: Using local file '~/scap-files/pub-projects-security-oval-
suse.linux.enterprise.15-patch.xml.bz2'
 instead of 'https://ftp.suse.com/pub/projects/security/oval/
suse.linux.enterprise.15-patch.xml.bz2'

 --- Starting Evaluation —
```

Tip

Download and use the specific files that are relevant for your SUSE Linux Enterprise product version, and avoid more generic ones. Being specific about the purpose and the files helps reduce the usage of server resources such as the processor, memory, storage and bandwidth. In addition, smaller file sizes also reduce the time required to complete the evaluation. For example, if you are interested only in SUSE Linux Enterprise 15 SP5, use the file available at https://ftp.suse.com/pub/projects/security/oval/suse.linux.enterprise.15-sp5-patch.xml.bz2↗.

4. *Optionally*, you can generate an HTML report from the XML results file.

```
> sudo oscap xccdf generate report ssg-sle15-xccdf-stig-results.xml >
ssg-sle15-xccdf-stig-report.html
```

Tip

You can generate an HTML report directly using the `oscap xccdf eval --report` option, but separating the scan and the HTML report generation leads to less usage of server resources.

7.5 Scanning and auditing systems using OVAL files

Using the OVAL content files for SUSE Linux Enterprise products, you can assess your SUSE Linux Enterprise systems and generate reports on the RPM package names and versions that are known to be affected by security issues in published CVEs.

The OVAL data provided by SUSE includes the following:

- The patch-style OVAL data, which expresses all security updates on a patch level. These can include multiple CVEs per patch.
- The vulnerability OVAL data, which expresses security vulnerabilities on a CVE level.

For detailed information on OVAL support provided by SUSE, refer to https://www.suse.com/support/security/oval/.

You can download OVAL files provided by SUSE from https://ftp.suse.com/pub/projects/security/oval/. As a best practice for scanning and auditing systems using OVAL files, perform the following procedure:

1. *(Optional)* Create a directory for downloading and storing remote resources.

```
> mkdir ~/oval-files (1)
```

(1) Directory to store downloaded remote resources such as OVAL patch files. If you have identified a suitable directory, skip this step.

2. Download the remote resource and save it as a local file.

```
> wget -O ~/oval-files/suse.linux.enterprise.15-patch.xml.bz2 (1) \
https://ftp.suse.com/pub/projects/security/oval/suse.linux.enterprise.15-
patch.xml.bz2 (2)
```

(1) The path to the locally saved file.

❷ The remote resource to be downloaded and saved locally.

3. Run the evaluation using the local files downloaded earlier from the remote source.

```
> sudo oscap oval eval \
--results sle15-oval-results.xml \
~/oval-files/suse.linux.enterprise.15-patch.xml.bz2 \

Definition oval:org.opensuse.security:def:45435: false
Definition oval:org.opensuse.security:def:45434: false
Definition oval:org.opensuse.security:def:45433: false
Definition oval:org.opensuse.security:def:45432: false
Definition oval:org.opensuse.security:def:45431: false
Definition oval:org.opensuse.security:def:45430: false
Definition oval:org.opensuse.security:def:45429: false
...

Evaluation done.
```

Tip

Download and use the specific files that are relevant for your SUSE Linux Enterprise product version, and avoid more generic ones. Being specific about the purpose and the files helps reduce the usage of server resources such as the processor, memory, storage and bandwidth. In addition, smaller file sizes also reduce the time required to complete the evaluation. For example, if you are interested only in SUSE Linux Enterprise 15 SP5, use the file available at https://ftp.suse.com/pub/projects/security/oval/suse.linux.enterprise.15-sp5-patch.xml.bz2.

4. *Optionally*, you can generate an HTML report from the XML results file.

```
> sudo oscap oval generate report results sle15-oval-results.xml >
sle15-oval-report.html
```

Tip

You can generate an HTML report directly using the **`oscap oval eval --report`** option, but separating the scan and the HTML report generation leads to less usage of server resources.

8 Vulnerability remediation

The security policy profiles in the `SCAP Security Guide` can not only be used to scan a target system and to generate reports, but also to automatically apply fixes to the target system (`remediation`), if possible.

Important: Automatic remediation not always available

Automatic remediation is *not* offered in case the automatic application of a fix is too dangerous to be enforced in a running target system.

8.1 OpenSCAP remediation process

OpenSCAP allows to automatically remediate target systems that have been found in a non-compliant state. This requires an XCCDF file with instructions. The overall process is as follows:

1. The **`oscap`** command-line tool performs a system scan.
2. Each rule that fails is marked as a candidate for remediation.
3. Within the XCCDF file, **`oscap`** then searches for an appropriate <xccdf:fix> element, resolves it, prepares the environment, and executes the fix script. The fix scripts can be either Bash `*.sh` files or Ansible playbook `*.yml` files.
4. After the execution of the script, the respective rule is evaluated again to check if the fix was successful.

All results of the remediation are stored in an output XCCDF file.

8.2 OpenSCAP remediation options

For remediating a target system with **`oscap`**, you have the following options:

Remediation on the fly

You can remediate a target system on the fly, while you are scanning it. In this case, evaluation and remediation are performed as a part of a single command. For details, see *Section 8.3.1, "Remediating SUSE Linux Enterprise (on the fly)"*.

Remediation after scanning

You can remediate a target system after you have scanned it. In the first step, the system is only evaluated, and the results are stored in the XCCDF results file. In the second step, `oscap` executes the fix scripts and verifies the result. For details, see *Section 8.3.2, "Remediating SUSE Linux Enterprise (after scanning)"*.

Review mode

The review mode allows to save remediation instructions to a file for further review. The remediation content is not executed during this operation. For details, see *Section 8.3.3, "Storing SLE remediation instructions for review"*.

8.3 Remediating a SLE system with `oscap`

The following examples show how to scan and remediate SUSE Linux Enterprise locally with `oscap` to comply with a certain profile.

8.3.1 Remediating SUSE Linux Enterprise (on the fly)

For remediation on the fly, use the `--remediate` command-line option.

EXAMPLE 2: REMEDIATING SLE 15 (ON THE FLY)

```
> sudo oscap xccdf eval --remediate❶ \
    --profile stig❷ \
    --results /tmp/results.xml❸ \
    /usr/share/xml/scap/ssg/content/ssg-sle15-ds.xml❹
```

❶ Calls the `oscap xccdf` module and tells it to perform an evaluation plus a remediation of the target system in one go.

❷ Specifies the profile to use, in this case, `stig`.

❸ Saves the results of the evaluation to `/tmp/results.xml`.

❹ Specifies the `SCAP Security Guide` policy file to use. In this example, we use a policy file in the `DataStream` format that applies to SUSE Linux Enterprise code 15. To list all available policies, run: `ls -1 /usr/share/xml/scap/ssg/content/ssg-*-ds.xml`. For more information about a particular policy, run `oscap info` on the file.

In the resulting `/tmp/results.xml` file, the first `TestResult` element shows the result of the scan *before* the remediation. The second `TestResult` element shows the result of the scan *after* applying the remediation. In the second `TestResult` element, if the result of a rule is `fixed`, this means that the fix was successfully applied, and this rule now passes evaluation. If the result of a rule is `error`, this means that the remediation for this rule was not successful, and the rule still does not pass evaluation.

8.3.2 Remediating SUSE Linux Enterprise (after scanning)

In this example, we first execute a scan and then run the remediation as next step.

EXAMPLE 3: REMEDIATING SLE (AFTER SCANNING)

1.
```
> sudo oscap xccdf eval ❶ \
      --profile stig ❷ \
      --results /tmp/results.xml ❸ \
      /usr/share/xml/scap/ssg/content/ssg-sle15-ds.xml ❹
```

   ❶ Calls the **`oscap xccdf`** module and tells it to perform an evaluation.

   ❷ Specifies the profile to use, in this case, `stig`.

   ❸ Saves the results of the evaluation as an XCCDF file to `/tmp/results.xml`.

   ❹ Specifies the `SCAP Security Guide` policy file to use. In this example, we use a policy file in the `DataStream` format that applies to SUSE Linux Enterprise code 15. To list all available policies, run: **`ls -1 /usr/share/xml/scap/ssg/content/ssg-*-ds.xml`**. For more information about a particular policy, run **`oscap info`** on the file.

   During this step, the system is only evaluated, and the results are stored in a `TestResult` element in `/tmp/results.xml`.

2.
```
> sudo oscap xccdf remediate ❶ \
    --results /tmp/results.xml ❷ \
    /tmp/results.xml ❸
```

   ❶ Calls the **`oscap xccdf`** module and tells it to perform a remediation.

   ❷ Saves the results of the remediation to `/tmp/results.xml`.

   ❸ Uses the `/tmp/results.xml` XCCDF file from the first step (evaluation) as input file.

> During this step, the results file from the first step is used as input for the **oscap** command. You can safely store the results from the second step in the same file that you use as input file, */tmp/results.xml*. During this run, **oscap** creates a new `xccdf:TestResult` element in the file. The new element is based on the previous one and inherits all the data. The newly created `xccdf:TestResult` element differs only in the `rule-result` elements which failed in the first run. Only for those is the remediation executed.

8.3.3 Storing SLE remediation instructions for review

You can also run **oscap** in review mode to store remediation instructions to a file for further review. During this operation, the remediation content is *not* executed. The following shows how to generate remediation instructions in the form of a shell script:

EXAMPLE 4: STORING SLE 15 REMEDIATION INSTRUCTIONS FOR REVIEW

```
> sudo oscap xccdf generate fix❶ \
    --template urn:xccdf:fix:script:sh❷ \
    --profile stig❸ \
    --output my-remediation-script.sh❹ \
    /usr/share/xml/scap/ssg/content/ssg-sle15-ds.xml❺
```

❶ Calls the **oscap xccdf** module and tells it to generate a file with remediation instructions.

❷ Specifies the template to use, in this case, a shell script.

❸ Specifies the profile to use, in this case, `stig`.

❹ Specifies the file to which the remediation instructions are written.

❺ Specifies the `SCAP Security Guide` policy file to use. In this example, we use a policy file in the `DataStream` format that applies to SUSE Linux Enterprise code 15. To list all available policies, run: **ls -1 /usr/share/xml/scap/ssg/content/ssg-*-ds.xml**. For more information about a particular policy, run **oscap info** on the file.

8.4 Remediating a SLE system with Ansible

You can use the Ansible playbooks provided by the `SCAP Security Guide` to remediate a local system.

The `ansible` package is available from `SUSE Package Hub`. Register your SUSE Linux Enterprise system and enable the `SUSE Package Hub` extension. For SUSE Linux Enterprise 12, you additionally need to enable the `Public Cloud` module. Then install the package with **`sudo zypper in ansible`**.

EXAMPLE 5: REMEDIATING SLE 15 WITH ANSIBLE

For example, to remediate your system using the STIG Ansible playbook for SUSE Linux Enterprise 15 provided by the `SCAP Security Guide`, use the following command.

Warning: System configuration changes

The following command alters the configuration of your system immediately. Make sure to test this thoroughly in a non-production system first.

```
> sudo ansible-playbook -i "localhost," -c local \
/usr/share/scap-security-guide/ansible/sle15-playbook-stig.yml
```

After the playbook has finished, you are prompted to log in to your system, which is now compliant to the chosen policy.

9 Related topics

- Check out the `SCAP Security Guide` pages online at https://www.open-scap.org/security-policies/scap-security-guide/.
- For general instructions on how to use the `SCAP Security Guide`, see the README in https://github.com/ComplianceAsCode/content/.
- Find the *OpenSCAP User Manual* at https://static.open-scap.org/openscap-1.2/oscap_user_manual.html.

10 Legal Notice

For SUSE trademarks, see https://www.suse.com/company/legal/. All third-party trademarks are the property of their respective owners. Trademark symbols (®, ™ etc.) denote trademarks of SUSE and its affiliates. Asterisks (*) denote third-party trademarks.

All information found in this book has been compiled with utmost attention to detail. However, this does not guarantee complete accuracy. Neither SUSE LLC, its affiliates, the authors nor the translators shall be held liable for possible errors or the consequences thereof.

GNU Free Documentation License

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or non-commercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or non-commercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

D. Preserve all the copyright notices of the Document.

E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

H. Include an unaltered copy of this License.

I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.

N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.

O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties--for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/ (https://www.gnu.org/copyleft/)↗.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

ADDENDUM: How to use this License for your documents

```
Copyright (c) YEAR YOUR NAME.
Permission is granted to copy, distribute and/or modify this document
under the terms of the GNU Free Documentation License, Version 1.2
or any later version published by the Free Software Foundation;
with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.
A copy of the license is included in the section entitled “GNU
Free Documentation License”.
```

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the “with...Texts.” line with this:

```
with the Invariant Sections being LIST THEIR TITLES, with the
Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.
```

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.