

SUSE Solution Security Risk Report 2024

All SUSE Products

Stoyan Manolov, Head of Solution Security (SUSE)

SUSE Solution Security is committed to delivering best-in-class software security to its customers and to the open source community. The primary objectives are to treat software security as an ongoing and continual process.

The goal of this report is to provide a summary of all security vulnerabilities which affected SUSE products in calendar year 2024.

Disclaimer: This document is part of the SUSE Best Practices series. All documents published in this series were contributed voluntarily by SUSE employees and by third parties. If not stated otherwise inside the document, the articles are intended only to be one example of how a particular action could be taken. Also, SUSE cannot verify either that the actions described in the articles do what they claim to do or that they do not have unintended consequences. All information found in this document has been compiled with utmost attention to detail. However, this does not guarantee complete accuracy. Therefore, we need to specifically state that neither SUSE LLC, its affiliates, the authors, nor the translators may be held liable for possible errors or the consequences thereof.

Contents

1	Motivation	4
2	Major security vulnerabilities in 2024	5
3	Vulnerability management in 2024	17
4	Securing our product portfolio	20
5	Commitment to customer trust and reliability	23
6	About SUSE	24
7	Forward-looking statements	25
8	Legal notice	26
9	GNU Free Documentation License	27

1 Motivation

SUSE Solution Security is committed to delivering best-in-class software security to customers and to the open source community. The primary objectives are to treat software security as an ongoing and continual process that never ends. This implies the following actions:

- Promptly react to security incidents and deliver premium quality security updates.
- Continuously improve the security-related functionality in SUSE products.
- Continuously contribute to the rapidly growing maturity of open source software.
- Respect the open source software security principles of openness, transparency and traceability.

The SUSE Security Team addresses all aspects of software security on an ongoing basis. Software security cannot be thought of as a state you can achieve at a specific point in time. Instead, it is a process that must be executed with professional expertise and continuous development. This persistent focus is what has given open source software, Linux and SUSE an excellent reputation for security. The SUSE Solution Security team is responsible for handling all SUSE product-related security incidents. In this team, clear and well-defined roles are assigned to track new incidents and coordinate needed updates. The team closely collaborates with all SUSE software engineer specialists.

The objective of this report is to provide a summary of all security vulnerabilities which affected SUSE products in calendar year 2024. We will go into details on the high-impact vulnerabilities and elaborate on how we responded to these incidents. For a better understanding of our classification mechanisms, we have described our rating system along with the equivalency of each rating to the CVSS v3.1 scoring calculator. Our Solution Security team has begun CVSS 4.0 scoring, and we will display both CVSS v3.1 and CVSS v4.0 on our CVE Web pages for your information and reference.

2 Major security vulnerabilities in 2024

2.1 CVE-2024-3094 (supply chain attack against xz)

Overview

SUSE received notification of a supply chain attack against the xz compression tool and liblzma library.

Security Researcher Andres Freund reported to Debian that the xz / liblzma library had been backdoored. Malicious code was discovered in the upstream tarballs of xz, starting with version 5.6.0. This backdoor was introduced in the upstream GitHub xz project with release 5.6.0 in February 2024. Through a series of complex obfuscations, the liblzma build process extracts a pre-built object file from a disguised test file existing in the source code, which is then used to modify specific functions in the liblzma code. This results in a modified liblzma library that, among other malicious functionalities, added a backdoor to allow the attacker arbitrary code execution via ssh.

Solution

To maintain product integrity, SUSE Linux Enterprise and openSUSE Leap are built in isolation from openSUSE Tumbleweed. This prevents the automatic inclusion of Tumbleweed's code, functionalities, and characteristics. Rigorous analysis has confirmed that the malicious file present in Tumbleweed is not incorporated into SUSE Linux Enterprise or Leap. Moreover, SUSE has verified that SUSE Linux Enterprise BCI, SUSE Rancher, SUSE Edge, and SUSE Multi-Linux Support (formerly SUSE Liberty Linux) remain unaffected. SUSE has not released xz versions 5.6.0 or 5.6.1 in any product offering other than openSUSE Tumbleweed. We will continue to monitor this situation and issue updates as necessary.

Following this incident, SUSE conducted internal and external brainstorming sessions to identify mitigations against supply chain attacks. A summary of these discussions is available on our [opensuse.org](https://www.opensuse.org/brainstorming) brainstorming page. We have already begun implementing several of these ideas, recognizing that no single solution fully eliminates such threats.

References

- openSUSE news:
<https://news.opensuse.org/2024/03/29/xz-backdoor> ↗
- Original email message:
<https://www.openwall.com/lists/oss-security/2024/03/29/4> ↗
- SUSE Web page for CVE-2024-3094:
<https://www.suse.com/security/cve/CVE-2024-3094> ↗
- openSUSE news:
<https://news.opensuse.org/2024/04/12/learn-from-the-xz-backdoor/> ↗
- openSUSE Wiki:
https://en.opensuse.org/XZ_backdoor_brainstorming ↗

2.2 CVE-2024-47177, CVE-2024-47175, CVE-2024-47176 and CVE-2024-47076 (remote code execution via cups-browsed)

Overview

A security researcher “evilsocket” has disclosed a chain of security vulnerabilities in CUPS and related tools.

When a **VZEROUPPER** instruction is discarded as part of a bad transient execution path, its effect on internal tracking is not unwound correctly. This manifests as the wrong micro-architectural state becoming architectural, and corrupting the vector registers.

Note: this vulnerability is unlikely to work across network gateway boundaries or any NATed setups.

SUSE does not enable the `cups-browsed.service` by default.

Possible workarounds

1. Block port 631 UDP in firewall if not already blocked.
2. Disable `cups-browsed.service` if it is running. Use

```
systemctl status cups-browsed.service
```

to verify the status and to stop and disable it:

```
systemctl stop cups-browsed.service  
  
systemctl disable cups-browsed.service
```

3. cups-browsed is part of the cups-filters RPM. If it is not required, an option is to remove the package:

```
zypper rm cups-filters
```

References

- openSUSE Wiki:
https://en.opensuse.org/SDB:CUPS_and_SANE_Firewall_settings ↗
- SUSE Support Knowledgebase article:
<https://www.suse.com/support/kb/doc/?id=000021571> ↗

2.3 CVE-2024-2201 (Branch History Injection aka InSpectre Gadget)

Overview

Security researchers from VU Amsterdam have identified a new class of transient execution attacks that can leak information from privileged OS parts, like the Linux kernel. The attack is a variant of, and an improvement on, the Spectre V2 attack.

The mitigation for the Linux kernel happens at the user/kernel boundary and it can use either hardware or software mitigations.

Note that software mitigations will reduce performance, depending on how many system calls are made from user space.

Solution

SUSE will provide kernel updates to mitigate this issue. Also, some CPU Microcode updates are required for the hardware mitigation. Please refer to the Intel documentation to get exact levels. SUSE will provide the latest Intel CPU Microcode releases when they become available.

The kernel mitigation can be configured with a kernel command-line option.

- spectre_bhi=off
Unconditionally disable the mitigation.
- spectre_bhi=on
Unconditionally enable the mitigation. If there is no hardware mitigation, the software mitigation will be enabled.
- spectre_bhi=auto
Enable the mitigation when the CPU supports the hardware mitigation and, if not, enable the software implementation for KVM hosts.

This option is also set from the “mitigations” global option.

Reporting

The mitigation status for BHI will be reported in the `/sys/devices/system/cpu/vulnerabilities/spectre_v2` sysfs file same as other Spectre V2 mitigations appended at the end of the current string with a comma (“,”) as a delimiter.

The following entries are possible:

- BHI: Not affected
System is not affected by BHI.
- BHI: IBRS
System is protected by the IBRS hardware mitigation.
- BHI: Retpoline
System is protected by the retpoline mitigation.
- BHI: BHI_DIS_S
System is protected by the BHI_DIS_S mitigation.
- BHI: SW loop
System is protected by the software clearing sequence.
- BHI: Vulnerable
System is vulnerable to BHI attacks.
Note that if there is no reference to BHI in the sysfs variable, it means the system is vulnerable.
- BHI: Vulnerable; KVM: SW loop

System is vulnerable to BHI attacks from user space; KVM is protected by a software clearing sequence.

References

- SUSE CVE-2024-2201
<https://www.suse.com/security/cve/CVE-2024-2201> ↗
- VUsec article:
<https://www.vusec.net/projects/native-bhi/> ↗
- Intel Developer Documentation:
<https://www.intel.com/content/www/us/en/developer/articles/technical/software-security-guidance/technical-documentation/branch-history-injection.html> ↗

2.4 CVE-2024-22030 (Man-in-the-middle (MITM) vulnerability exploitable in Rancher)

Overview

A newly discovered vulnerability within Rancher and Fleet, currently deemed a medium to high severity CVE-2024-22030, can be exploited in narrow circumstances through a man-in-the middle attack. An attacker would need to have control of an expired domain or execute a DNS spoofing/hijacking attack against the domain in order to exploit this vulnerability. The targeted domain is the one used as the Rancher URL. SUSE is not aware of any commercial exploitation of the described vulnerability, which has a high complexity bar for exploitation. Below, please find the advised remediation for all Rancher customers and users.

The described vulnerability is difficult to exploit, and certain external conditions, outside the control of the Rancher server, must be met and executed by a malicious actor. These are:

1. An attacker can hijack the domain used to register Rancher (the server-url of the Rancher cluster) or can execute a DNS hijacking or spoofing of that domain.
2. An attacker can generate a valid certificate for the targeted domain/DNS.
3. The certificate is valid and generated by a trusted CA that is also in the trust store of the targeted Rancher server; or the valid certificate is generated by a valid CA that was previously configured in the Rancher installation.

If an attacker succeeds with steps 1 and 2, and if 3 is a match, then the weakness in the Rancher and Fleet agent's CA data check can be exploited.

Note: Customers and users using certificates signed by their own private CAs do not seem to be affected by this issue, as long as their CA signing key is not leaked.

Solution

To remediate the issue, SUSE Rancher customers and users should follow standard security practices, including:

- Make sure to properly control the expiration and ownership of the domain used as the Rancher URL (the server-url of the Rancher cluster).
- Evaluate enabling DNSSEC as a way to protect against DNS spoofing or hijacking attacks.
- Monitor attempts to hijack the domain and DNS.
- Monitor attempts to create rogue certificates against your domain and the Rancher URL.
- Services like crt.sh and other monitors, from the Certificate Transparency (CT) project, are good places to watch for rogue certificates.
- Properly clean up and decommission unused clusters and downstream clusters, instead of leaving them behind. For example, downstream clusters which are alive while the main Rancher server is no longer available.
- See more information about how to remove Rancher components from a cluster, for the cases where decommissioning the entire cluster is not an option.

References

- Rancher security update:
<https://www.suse.com/c/rancher-security-update/> ↗
- Rancher Manager CVE:
https://ranchermanager.docs.rancher.com/reference-guides/rancher-security/security-advisories-and-cves?_gl=1*fw7j8m*_gcl_au*NDQwNjcwOTI5LjE3MzYxNjUwMzA.*_ga*MTY3NDExM-DUXMS4xNzE5OTExNzI3*_ga_JEVBS2XFKK*MTc0MjgwNjczNi4xMTEuMS4xNzQyODA5ND-k0LjYwLjAuMA.. ↗

2.5 CVE-2022-25375, CVE-2022-48837, CVE-2022-48926, CVE-2023-23559 (Security vulnerabilities in the Linux Kernel RNDIS driver)

Overview

The Linux Kernel RNDIS driver is considered unsafe, but currently left in the tree due to a large amount of users.

It is, however, not recommended to use it anymore, as it is considered insecure.

For this reason, SUSE has blocked the rndis module from loading to eliminate this attack surface.

Solution

Blocklisting is achieved by these lines:

```
/lib/modprobe.d/50-blacklist-rndis.conf:blacklist rndis_wlan  
/lib/modprobe.d/50-blacklist-rndis.conf:blacklist usb_f_rndis  
/lib/modprobe.d/50-blacklist-rndis.conf:blacklist rndis_host
```

If the module is loaded manually by the administrator, it is likely exploitable by local users.

If one or more of the above modules should be loaded automatically again, please remove the above lines or remove the /lib/modprobe.d/50-blacklist-rndis.conf file.

Reference

- SUSE Support Knowledgebase article:
<https://www.suse.com/support/kb/doc/?id=000021587> 

2.6 CVE-2023-52564 and CVE-2023-6546 (Security vulnerability in the Linux kernel n_gsm line discipline)

Overview

Security researchers have identified problems in the Linux kernel's n_gsm serial line discipline, which can be exploited by local attackers to gain elevated privileges.

Solution

SUSE has applied a patch to the n_gsm line discipline that only allows it to be used as root user, and considers removing it from future kernel updates, service packs and products.

The last reported problems currently have no CVE assigned by the Linux Kernel CNA yet due to process reasons, but might assign one later. Hence, the above CVE announcements point to the currently known CVEs only and will be updated as soon as possible.

SUSE has released fixed kernel packages for its distributions:

SLES 15 SP4 LTSS, SLE Micro 5.3, 5.4:

Default kernel: 5.14.21-150400.24.116.1 and newer

SLE Micro 5.3, 5.4:

RT kernel: 5.14.21-150400.15.76.1 and newer

Workaround

```
rmmod n_gsm
echo "blacklist n_gsm" >> /etc/modprobe.d/99-n_gsm_blacklist.conf
echo "install n_gsm /bin/true" >> /etc/modprobe.d/99-n_gsm_blacklist.conf
```

To disallow auto-loading of tty line discipline modules in general:

```
sysctl dev.tty.ldisc_autoload = 0
```

Reference

- SUSE Support Knowledgebase article
<https://www.suse.com/support/kb/doc/?id=000021437> 

2.7 CVE-2023-28746 (Register File Data Sampling (RFDS))

Overview

Security researchers have identified yet another CPU transient execution information leak, allowing information extracted from various register filesets, like floating-point registers, vector registers and integer registers.

This vulnerability only affects Intel Atom processors (aka XEON E cores).

Solution

Please install the update that contains the respective fix for this issue.

1. To retrieve the specific patch name, please use:

```
zypper lp -a --cve=CVE-2023-28746
```

2. Use the following command to apply the patch:

```
zypper in -t patch <name_of_patch>
```

The following options influence the mitigation:

- reg_file_data_sampling=on
If the CPU is vulnerable and fixed microcode is available, enables the mitigation.
- reg_file_data_sampling=off
Disables the mitigation.

This flag is also set by the generic “mitigations” option.

Reporting

A new reporting file was added:

```
/sys/devices/system/cpu/vulnerabilities/reg_file_data_sampling
```

This file can have the following contents:

- Not affected
The CPU is not affected by the problem.
- Vulnerable
The CPU is vulnerable, but no mitigation is enabled.
- Vulnerable: No microcode
The CPU is vulnerable, but the CPU microcode is not updated.
- Mitigation: Clear Register File
The CPU is vulnerable and the CPU buffer clearing mitigation is enabled.

Reference

- SUSE Support Knowledgebase article:
<https://www.suse.com/support/kb/doc/?id=000021404> ↗

2.8 CVE-2023-1281, CVE-2023-1829 and CVE-2021-47295 (Security vulnerabilities in the Linux kernel cls_tcindex driver)

Overview

The Linux kernel `cls_tcindex` driver has multiple security issues that are hard to fix. Since there are few users of the module, SUSE has blocked the `cls_tcindex` module from loading to eliminate this attack surface.

Solution

The blocklisting is achieved by this line:

```
/lib/modprobe.d/50-blacklist-netcls.conf:blacklist cls_tcindex
```

If the module is loaded manually by the administrator, it is likely exploitable by local users. If the module should be loaded automatically again, please comment on/remove the above line or remove the `/lib/modprobe.d/50-blacklist-netcls.conf` file.

SUSE Linux Enterprise Server 15 SP6 and newer kernels no longer include `cls_tcindex` and SUSE is not planning to backport future security fixes for `cls_tcindex` at this time.

References

- SUSE Support Knowledgebase article:
<https://www.suse.com/support/kb/doc/?id=000021588> 

2.9 CVE-2023-21400, CVE-2023-3609, CVE-2022-32250, CVE-2022-29582, CVE-2022-27666, CVE-2022-2588, CVE-2022-0995, CVE-2021-4157 and CVE-2021-3492 (Linux kernel memory corruption vulnerabilities exploitable through the SLUBStick technique)

Overview

Researchers from the Graz University of Technology have recently released a paper in which they present how they were able to take heap memory corruption vulnerabilities and memory allocation flaws in the Linux kernel, such as out-of-bounds writes, use-after-frees and double-frees, and, together with a sophisticated multiple-stage technique developed by them, use such vulnerabilities to achieve arbitrary read and write capabilities in a vulnerable system. Threat actors can therefore use such a technique to turn what would otherwise be limited read and write capabilities with a small impact into attacks that can gravely compromise a system.

The SLUBStick technique achieves such an objective by manipulating the Linux kernel's SLUB memory allocator in specific ways. This allows an attacker to perform reliable cross-cache attacks that deliver better results than other known techniques, which would usually only lead to system crashes rather than allow for code execution. This reliability improvement comes from the timing side-channel approach proposed by the researchers. A memory corruption vulnerability can then be transformed into a page table entry rewrite, which allows an attacker to map any physical memory in the system into their address space, giving them the arbitrary read and write capabilities that can lead to other more serious consequences.

To successfully exploit a vulnerability through the use of the SLUBStick technique, an attacker needs local access to the target machine, as well as privileges that would allow them to execute code in this same machine. Finally, the Linux kernel in such a machine must contain an unpatched heap memory corruption vulnerability that could be exploited.

Solution

SUSE products (both under general and under LTSS support) that could potentially be attacked through the use of the SLUBStick technique have already been fixed for the related vulnerabilities and, therefore, no longer are at risk when it comes to the example cases presented in the research.

SUSE is also taking continuous action to fix memory corruption vulnerabilities affecting the Linux kernel as they are reported. In this way, SUSE products stay hardened and protected against any additional vulnerabilities that might be exploitable through the SLUBStick technique.

Keeping systems updated with the latest kernel patches should provide sufficient protection against this issue.

SLUBStick is not a security vulnerability in itself, it is a technique that makes exploitation of other vulnerabilities easier. Hence, SLUBStick is not assigned a CVE number and mitigation happens through fixing other vulnerabilities that could be potentially exploited by this technique.

References

- SUSE Support Knowledgebase article:
<https://www.suse.com/support/kb/doc/?id=000021529> ↗
- SUSE CVE-2023-21400:
<https://www.suse.com/security/cve/CVE-2023-21400.html> ↗
- SUSE CVE-2023-3609
<https://www.suse.com/security/cve/CVE-2023-3609.html> ↗
- SUSE CVE-2022-32250
<https://www.suse.com/security/cve/CVE-2022-32250.html> ↗
- SUSE CVE-2022-29582
<https://www.suse.com/security/cve/CVE-2022-29582.html> ↗

- SUSE CVE-2022-27666
<https://www.suse.com/security/cve/CVE-2022-27666.html>
- SUSE CVE-2022-2588
<https://www.suse.com/security/cve/CVE-2022-2588.html>
- SUSE CVE-2022-0995
<https://www.suse.com/security/cve/CVE-2022-0995.html>
- SUSE CVE-2021-4157
<https://www.suse.com/security/cve/CVE-2021-4157.html>
- SUSE CVE-2021-3492
<https://www.suse.com/security/cve/CVE-2021-3492.html>

3 Vulnerability management in 2024

The SUSE Solution Security team constantly monitors all the software components used in our products for security issues. More and improved tools are now available to find zero-day vulnerabilities and scan for existing vulnerabilities. Such tools can check and report whether the application code written conforms to standard security best practices or whether there are major holes in potential attack vectors such as buffer overflow, denial of service, or unwanted elevated access. It is clear that developers are becoming more and more security-aware and that the quality of the code being developed has improved significantly, both in quantity and quality. While we are seeing an increasing number of important vulnerabilities, the number of critical vulnerabilities is decreasing year after year.

TABLE 1: VULNERABILITIES WITH A UNIQUE CVE IDENTIFIED, IMPACTING SUSE PRODUCTS IN 2024

Low	Moderate	Important	Critical
318	2997	603	16

TABLE 2: SECURITY UPDATES AND PATCHES RELEASED TO FIX THESE VULNERABILITIES IN 2024

Low	Moderate	Important	Critical
392	1480	2229	52

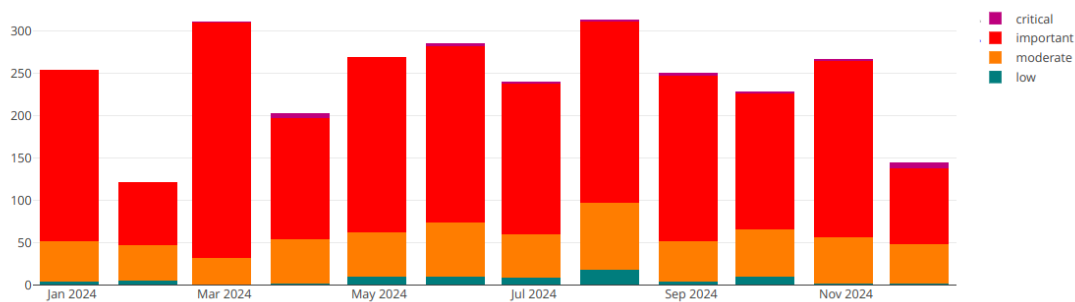


FIGURE 1: SECURITY UPDATES AND PATCHES RELEASED PER MONTH IN 2024

3.1 What's new in 2024: An increased amount of reported kernel security vulnerabilities

In 2024, the National Vulnerability Database (NVD) experienced a significant surge in reported security vulnerabilities. This increase is largely attributed to the Linux kernel team, which, via its own CVE Numbering Authority (CNA), has recently begun issuing CVEs for a broader range of kernel issues. Their inclusive approach, covering diverse kernel use-cases from embedded systems to enterprise deployments, results in the issuance of many CVEs that do not impact SUSE Linux product usage. Nonetheless, SUSE engineers addressed over 4,000 unique CVEs affecting various kernel versions in 2024.

A significant number of allocated CVEs do not pose an exploitable risk within SUSE Linux kernels. In alignment with industry standards, SUSE will not address CVEs falling under the following categories:

- Code SUSE does not build into its kernels
CVEs targeting code that is not enabled in SUSE kernels through CONFIG options. That includes drivers which are not enabled but also debugging code like VM_BUG_ON etc.
- Testing infrastructure
Fixes for tools or test scenarios that are not meant to be run on production systems.
- WARN_ON fixes
SUSE default and recommended configurations, which only trigger warnings due to disabled **panic_on_warn**.
- Small GFP_KERNEL allocation failures triggering **NULL ptr**

Fixes adding allocation failure checks to prevent from NULL ptr crashes for very small allocations. If the allocation request is GFP_KERNEL and the allocation size is small (\leq PAGE_ALLOC_COSTLY_ORDER), then an allocation failure is practically impossible. This means that those fixes are never tested and, therefore, are risky to introduce, potentially leading to unwanted side effects that would be harder to notice. The benefit of the fix is therefore much smaller than the risk fixing it might cause.

- debugfs only fixes

debugfs, a kernel debugging interface, lacks the rigorous API/ABI scrutiny applied to other kernel functionalities. Consequently, enabling debugfs is discouraged, especially on production systems. If required, access should be strictly limited to privileged users. On SUSE systems, debugfs access is restricted to root only.

- Boot time crashes

Fixes for boot time crashes, either because of an unexpected HW configuration (LPAR configurations, device tree misconfiguration, BIOS/FW bugs) or because of kernel command line misconfiguration.

- Memory leaks that cannot be directly triggered from the user space

CVEs assigned for memory leaks, which are either impractical to trigger (for example, clean up not done on module unloading) or on a failure path which is not controllable by an attacker.

- Hardware-specific failure trigger

Kernel crashes triggered by a HW failure are not considered a security threat unless they can be directly triggered by a user.

Note that some failure modes are generally not recoverable and the only effective protection is physical inaccessibility (for example, storage connectivity) but there are use cases which are primarily focused on the third-party HW controlled by potential attacker (for example, USB stick kiosk). The latter is considered a real security attack vector, while the former is not.

SUSE will also decide on a case-by-case basis about:

- Issues triggered solely by system root/CAP_SYSADMIN

If a crash/use-after-free (UAF) or similar issue is only triggered by a privileged user, those fixes are not considered security relevant because such a user can already compromise the security of the system. This would include interfaces like fault injection (for example, HW poisoning), sysctl/sysfs/proc configurations that might trigger crashes/UAF etc, kernel modules loading and unloading and many others.

For untrusted root scenarios (kernel lockdown, for example, in secure boot) issues which allow to bypass lockdown, constraints are considered security relevant.

Issues which SUSE will not fix are marked as “Won't Fix” on the SUSE CVE Web pages.

4 Securing our product portfolio

4.1 Proactive review of code

Our skilled team of security engineers regularly reviews the code we ship. We harden our products and conduct security audits on selected packages. Packages and products are continually reviewed to ensure we protect our customers' systems with the latest state-of-the-art technology. To this end, we have introduced an automation setup that notifies our team of potentially dangerous changes in existing or new packages (for example, important permission changes) and triggers an audit if necessary.

Over the last year, our proactive Security team has found and assigned CVE IDs to a number of vulnerabilities which document the more important findings. Find more information on our [blog page \(https://security.opensuse.org/\)](https://security.opensuse.org/) ↗.


4.2 CSAF and OSV security advisory data


The Common Security Advisory Format (CSAF) is an industry-standard format for publishing security advisories in machine readable form.

SUSE currently offers:

- CSAF data indexed by Security Advisory in CSAF 2.0 format.
- CSAF VEX data indexed by CVE in CSAF 2.0 VEX format.

SUSE has started generating CSAF data for SUSE security update notifications and CVEs in February 2023, including all previous security advisories and CVEs.


The CSAF 2.0 security advisory data can be downloaded from this SUSE ftp site (<https://ftp.suse.com/pub/projects/security/csaf/>) .

The CSAF 2.0 VEX data indexed by CVE can be downloaded from this SUSE ftp site (<https://ftp.suse.com/pub/projects/security/csaf-vex/>) .

The data is available under the Creative Commons license, with attribution CC-BY-4.0. The CSAF format is a verbose and simple JSON format, so it can be hooked into other tools pretty easily even without additional libraries.

A list of reference tools (<https://oasis-open.github.io/csaf-documentation/tools.html>)  is also provided by OASIS.

The Open Source Vulnerabilities (OSV) is a Google-based vulnerability database and triage infrastructure for open source projects aimed at helping both open source maintainers and consumers of open source.




SUSE also publishes regularly updated OSV data, available at: <https://ftp.suse.com/pub/projects/security/osv/> .

4.3 SUSE received first FIPS 140-3 cryptographic certificates

After several years of work, the NIST CMVP agency has improved upon the existing FIPS 140-2 certification and established the FIPS 140-3 certification. The new standard brings many changes that are described in the **Implementation Guidance**. They implemented new cryptographic primitive lifecycle requirements and expanded self-test capabilities. Furthermore, they enhanced memory integrity and streamlined the certification process.

SUSE was the first Linux vendor to receive FIPS 140-3 certificates for its cryptographic modules based on SUSE Linux Enterprise 15 SP4 and related products.

SUSE has received the following certificates:

- SUSE Linux Enterprise GnuTLS Cryptographic Module (<https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4742>) 
- SUSE Linux Enterprise NSS Cryptographic Module (<https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4728>) 
- SUSE Linux Enterprise Kernel Crypto API Cryptographic Module (<https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4727>) 

- This certificate covers the kernel default and RT flavors.
- SUSE Linux Enterprise OpenSSL Cryptographic Module (<https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4725>) ↗
- This certificate covers the system OpenSSL library version 1.1.1.
- SUSE Linux Enterprise Libgcrypt Cryptographic Module (<https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4722>) ↗
- These certificates cover the 4 CPU architectures supported by SUSE Linux Enterprise 15 (Intel and AMD x86_64, IBM Z (s390x), IBM Power (ppc64le) and ARM aarch64).

SUSE at this time is working on certifying the cryptographic modules of SUSE Linux Enterprise Server 15 SP6, and is already listed on the [Implementation under Test](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/modules-in-process/iut-list) (<https://csrc.nist.gov/Projects/cryptographic-module-validation-program/modules-in-process/iut-list>) ↗ list.

4.4 Adoption of SELinux in openSUSE Tumbleweed, SUSE Linux Micro 6.x and SUSE Linux Enterprise 16

We recently announced that for openSUSE Tumbleweed, the default mandatory access control (MAC) system selected by the installer will be switched from AppArmor to SELinux in enforcing mode. Additionally, the openSUSE Tumbleweed minimal VM is shipped with SELinux in enforcing mode.

Users installing openSUSE Tumbleweed via the ISO image will see SELinux in enforcing mode as a default option in the installer. If the user prefers to use AppArmor instead of SELinux, they can change the selection to AppArmor manually in the installer.

AppArmor continues to be excellently maintained by Christian Boltz (@cboltz) as before.

Existing installations using AppArmor will **not** be migrated. In case the user wishes to migrate manually to SELinux, a guide is provided on the openSUSE Wiki in the Reference links below.

Following this model in our enterprise-grade solutions, we have switched to SELinux in our SUSE Linux Micro 6.x family and we will use SELinux as the default MAC system in the upcoming release of SUSE Linux Enterprise 16.

Reference

- openSUSE Wiki article:
https://en.opensuse.org/Portal:SELinux/Setup#Setup_SELinux_on_existing_Tumbleweed_systems ↗

5 Commitment to customer trust and reliability

January 16th 2024

SUSE has achieved certification by the Chinese government for SUSE Linux Enterprise 15 for the GB 18030 standards. The GB 18030 is the Chinese ideographic character set and encoding standard mandated by the Chinese government. It was updated in 2022, supports the extended character support, and was implemented on August 1, 2023.

January 17th 2024

The University of New Hampshire Interoperability Laboratory (UNH-IOL) has certified [SUSE Linux Enterprise Server 15 SP5 \(SLES 15 SP5\)](#) under the [USGv6R1 \(https://www.iol.unh.edu/registry/usgv6/877/sdoc\)](https://www.iol.unh.edu/registry/usgv6/877/sdoc) ↗ technical requirements, and under the IPv6 Ready Logo Program (<https://www.ipv6ready.org/db/index.php/public/logo/02-C-002792/>) ↗.

January 18th 2024

The University of New Hampshire Interoperability Laboratory (UNH-IOL) has certified [SUSE Linux Enterprise Micro \(SLE Micro\) 5.5](#) under the [USGv6 R1 \(https://www.iol.unh.edu/registry/usgv6/880/sdoc\)](https://www.iol.unh.edu/registry/usgv6/880/sdoc) ↗ technical requirements, and under the IPv6 Ready Logo Program (<https://www.ipv6ready.org/db/index.php/public/logo/02-C-002818/>) ↗.

January 19th 2024

SUSE has successfully obtained renewed certifications for ISO 27001 and ISO 27701 from NQA. These renewed certifications serve as a testament to SUSE's ongoing dedication to excellence, providing our customers with the assurance that our practices meet the highest industry and compliance standards.

You can download the renewed certifications by accessing the below links:

- ISO 27001 (<https://www.suse.com/assets/SUSE-27001-185587.pdf>) ↗
- ISO 27701 (<https://www.suse.com/assets/SUSE-27701-185588.pdf>) ↗

April 21st 2024

SUSE has received NIST validation under FIPS 140-2 for its SUSE Rancher Kubernetes Cryptographic Library. The certificate can be reviewed at: <https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4691>.

June 20th 2024

DISA has released the SUSE Linux Enterprise Micro (SLEM) 5 Security Technical Implementation Guide (STIG). The STIG can be downloaded from the DISA Document Library at: https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_SLEM_5_V1R1_STIG.zip.

August 20th 2023

SUSE has attained a Common Criteria EAL4 level security certification for SUSE Linux Enterprise Server 15 from the Korean Information Technology Security Certification Center (ITSCC) that evaluates and certifies products for use by government agencies of the Republic of Korea. SUSE Linux Enterprise Server 15 is now listed on the [ITSCC Approved Product Database](https://www.suse.com/assets/SUSE-27001-185587.pdf) (<https://www.suse.com/assets/SUSE-27001-185587.pdf>), permitting all agencies and organizations to use our product. The certificate can be viewed or retrieved from <https://www.itscc.kr/cert-prod/listA.do>.

October 7th 2024

SUSE has attained NIST FIPS 140-3 certification of our SUSE Linux Enterprise Server Libica Cryptographic Module, thus completing the full certification process of SLES 15 SP4.

December 17th 2024

SUSE Linux Micro 6.1 has been certified by the University of New Hampshire Interoperability Laboratory (UNH-IOL) against the technical requirements of the USGv6-r1 profile. UNH-IOL provides testing and evaluation services of IPv6 technologies and certifies compliance.

6 About SUSE

SUSE is a global leader in innovative, reliable and secure enterprise open source solutions, including SUSE Linux Suite, SUSE Rancher Suite, SUSE Edge Suite and SUSE AI Suite. More than 60% of the Fortune 500 rely on SUSE to power their mission-critical workloads, enabling them to innovate everywhere — from the data center to the cloud, to the edge and beyond. SUSE puts the “open” back in open source, collaborating with partners and communities to give customers the agility to tackle innovation challenges today and the freedom to evolve their strategy and solutions tomorrow. For more information, visit <https://www.suse.com>.

7 Forward-looking statements

Any statements in this document about future expectations, plans and prospects for the company, including statements containing the words “aims”, “targets”, “will”, “believes”, “anticipates”, “plans”, “expects”, and similar expressions, may constitute forward-looking statements and should be read with caution.


Actual results may differ materially from those indicated by such forward-looking statements as a result of various important factors, including competitive landscape, development of customer deals, reliance upon customer relationships, management of growth and acquisitions, the possibility of undetected software issues, the risks of impacts of the COVID-19 pandemic and economic downturns, pricing pressures and the viability of the Internet. In addition, any forward-looking statements included herein represent views as of the date of this document's release and these views could change. The Company does not have any obligation to update its forward-looking statements.

These forward-looking statements are subject to change and should not be relied upon as representing the Company's views as of any date other than the publication date of this document.

8 Legal notice

Copyright ©2006-2025 SUSE LLC and contributors. All rights reserved.

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or (at your option) version 1.3; with the Invariant Section being this copyright notice and license. A copy of the license version 1.2 is included in the section entitled “GNU Free Documentation License”.

SUSE, the SUSE logo and YaST are registered trademarks of SUSE LLC in the United States and other countries. For SUSE trademarks, see <http://www.suse.com/company/legal/> . Linux is a registered trademark of Linus Torvalds. All other names or trademarks mentioned in this document may be trademarks or registered trademarks of their respective owners.

Documents published as part of the **SUSE Best Practices** series have been contributed voluntarily by SUSE employees and third parties. They are meant to serve as examples of how particular actions can be performed. They have been compiled with utmost attention to detail. However, this does not guarantee complete accuracy. SUSE cannot verify that actions described in these documents do what is claimed or whether actions described have unintended consequences. SUSE LLC, its affiliates, the authors, and the translators may not be held liable for possible errors or the consequences thereof.

Below we draw your attention to the license under which the articles are published.

GNU Free Documentation License

Copyright (C) 2000, 2001, 2002 Free Software Foundation, Inc. 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA. Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

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. Secondly, 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 noncommercially, 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/>.

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.