SUSE

SUSE Best Practices

Security

SUSE Solution Security Risk Report 2025

All SUSE Products

Stoyan Manolov, Head of Solution Security (SUSE)

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 2025.

Contents

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 2025. 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 2025

2.1 Race condition in Apache Tomcat (CVE-2024-56337, CVE-2024-50379)

Overview

The CVE-2024-50379 security issue references an issue that could happen during JSP compilation on case-insensitive file systems, when the default servlet is enabled for write (not the default setting).

Users running Tomcat on case-insensitive file systems with the default servlet write-enabled (**`readonly`** initialization parameter set to `false`) may require additional configuration to fully mitigate CVE-2024-50379. The specific requirements depend on the version of Java being used with Tomcat:

- Running on Java 8 or Java 11: The system property `sun.io.useCanonCaches` must be explicitly set to `false` (it defaults to `true`).
- Running on Java 17: The system property `sun.io.useCanonCaches`, if set, must be set to `false` (it defaults to `false`).
- Running on Java 21 onwards: No further configuration is required (the system property and the problematic cache have been removed).

Solution

Future Tomcat versions will include checks that `sun.io.useCanonCaches` is set appropriately before allowing the default servlet to be write-enabled on a case-insensitive file system. Tomcat will also set `sun.io.useCanonCaches` to `false` by default where it can.

References

- https://www.suse.com/security/cve/CVE-2024-50379
- https://www.suse.com/security/cve/CVE-2024-56337

2.2 Branch Privilege Injection aka CVE-2024-45332

Overview

Security researchers at ETH Zurich found a new Spectre v2 transitional execution attack in Intel CPUs.

By exploiting Branch Predictor Race Conditions (BPRC), where some branch predictions persist over switching privilege boundaries in the processor, it allowed attackers from lower privileged processes to read data of higher privileged ones.

Solution

Existing mitigations need to be enhanced by updated Intel CPU Microcode, release 20250512 or higher.

References

- https://comsec.ethz.ch/research/microarch/branch-privilege-injection/
- https://www.suse.com/security/cve/CVE-2024-45332
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01247.html

2.3 CVE-2025-8671: HTTP/2 'MadeYouReset' DoS attack

Overview

Researchers from the Tel Aviv University have recently discovered a vulnerability in several HTTP/2 implementations, which can be exploited to cause denial of service in applications that depend on these implementations. The vulnerability, which was assigned CVE-2025-8671, is now known as 'MadeYouReset'.

Solution

Several upstream projects updated their code to implement a fix for the issue, and also provided patches that allow the vulnerability to be addressed in versions of their software shipped with SUSE products.

The following packages were affected:

- `netty`
- `jetty`
- `tomcat`

The 'MadeYouReset' vulnerability is caused by a flaw in HTTP/2 implementations where a stream reset is treated as a stream close operation, yet the server continues to process the stream. By sending continuous reset requests to a target server, an attacker can overload it because the requests are still processed, even though the reset streams are considered closed at the protocol level.

This is not a flaw in the HTTP/2 protocol itself, but rather in specific implementations. In HTTP/2, both the client and server are permitted to close streams at any time. Certain implementations, however, continue to process requests and generate responses even when those responses cannot be sent back to the client because the stream is considered closed. This creates a mismatch where the number of active HTTP requests being processed by the back-end does not align with the number of streams considered active from a protocol perspective. Consequently, by opening streams and rapidly triggering resets—via malformed frames or flow control errors—an attacker can exploit this mismatch. The server then attempts to handle an unbounded number of concurrent requests on a single connection, leading to resource exhaustion.

When targeted, a server will either exhaust its memory or its processing capabilities, which can lead to a crash (rendering the service completely offline), or to a limit on the number of client connections that can be handled at a given time (making the service intermittent and causing long response times).

The 'MadeYouReset' vulnerability is similar to, but not the same as, the 'RapidReset' vulnerability (CVE-2023-44487, https://www.suse.com/support/kb/doc/?id=000021240). Information on 'MadeYouReset' was publicly disclosed on August 13, 2025; prior to this date, there was no record of any 'MadeYouReset' attacks occurring in the wild.

References

- https://www.cve.org/CVERecord?id=CVE-2025-8671
- https://www.cve.org/CVERecord?id=CVE-2025-48989
- https://kb.cert.org/vuls/id/767506
- https://www.suse.com/security/cve/CVE-2025-8671.html
- https://www.suse.com/security/cve/CVE-2025-48989.html
- https://www.suse.com/security/cve/CVE-2025-55163.html
- https://www.suse.com/security/cve/CVE-2025-5115.html

2.4 CVE-2019-11135: TSX Asynchronous Abort (TAA)

Overview

Security researchers have found a side-channel information disclosure attack against Intel Transactional Synchronization Extensions (Intel TSX) Asynchronous Abort. During TSX transactions, when an asynchronous abort occurs, data may have already been fetched from memory addresses, making it available for side-channel attacks against microarchitectural buffers—such as store, load, or fill buffers. The scope of this exposure is similar to the Microarchitectural Data Sampling (MDS) attack disclosed in May 2019, and can leak small amounts of very recently accessed data.

Which processors are affected?

All Intel processors supporting TSX shipped to date are affected, including those with existing fixes for “Microarchitectural Data Sampling”. Refer to Intel's official documentation for the complete list of affected processors.

Solution

SUSE has released software updates to mitigate these issues. Future Intel processors will have this vulnerability mitigated at the hardware level.

How to detect presence of the problem?

A new `sysfs` variable was added to the CPU vulnerabilities:

`/sys/devices/system/cpu/vulnerabilities/tsx_async_abort`

This can contain the following states:

- *Not affected*
  The CPU is not affected by this problem.
- *Vulnerable*
  The CPU is affected by this vulnerability, and neither the CPU microcode nor kernel mitigations are applied.
- *Vulnerable: Clear CPU buffers attempted, no microcode*
  The kernel mitigations are present and active, but the CPU microcode does not support the buffer-clear operation. (This can also occur if the ability to clear CPU buffers is not reported to a guest VM.)
- *Mitigation: Clear CPU buffers*
  The software mitigation clearing the buffers using "VERW" is in use.
- *Mitigation: TSX disabled*
  The mitigation is that TSX has been disabled on the kernel command line during boot.

The following software mitigations are available:

- Switching off TSX support:
  Up to now TSX could not be disabled, but Intel has provided CPU Microcode updates for current CPUs that allow disabling TSX.
  This can be controlled by a Linux kernel boot command line option.
  - **`tsx=on`**
    Enable TSX support. This was the default until SUSE Linux Enterprise Server 15 SP5; however, throughout SP6 and SP7, the default has changed several times. Review the list of kernel versions at the end of this document for details.
  - **`tsx=off`**
    Disable TSX. Note that this only works on CPUs that support the option "IA32_TSX_CTRL", either when included on the silicon or via CPU Microcode Update.
  - **`tsx=auto`**
    If the TAA bug is present, TSX will be disabled. If not, TSX will stay enabled. Starting with certain kernel releases, this is now the new default. Refer to the list at the end of this document for details.

If TSX is disabled, the secondary mitigation below is not needed.

- Mitigations using VERW and Hyperthreading adjustments
  These adjustments are similar to those for the “MDS” attack. Note that using VERW buffer flushing is also required on CPUs where “MDS” is already addressed in hardware, and it requires accompanying CPU microcode.
  The kernel boot commands to control it are:

  - **`tsx_async_abort=off`**
    The TAA mitigation is disabled.

  - **`tsx_async_abort=full`**
    The TAA mitigation is enabled. If TSX is enabled, it will use the clear buffer mitigation. (This is the current SUSE Default.)

  - **`tsx_async_abort=full,nosmt`**
    The TAA mitigation is enabled. If TSX is enabled, it will use the clear buffer mitigation. Additionally, Hyperthreading is disabled to avoid potential cross hyperthread leakage.

References

- https://software.intel.com/security-software-guidance/insights/deep-dive-intel-transactional-synchronization-extensions-intel-tsx-asynchronous-abort
- https://www.suse.com/security/cve/CVE-2019-11135.html

2.5 CVE-2025-11561: Default Kerberos configuration allows privilege escalation on AD-joined Linux systems

Overview

The Kerberos local authentication plugin (`sssd_krb5_localauth_plugin`) is not enabled by default in the SSSD configuration.

Because of this, when the integration of Active Directory and the System Security Services Daemon (SSSD) occurs on Linux systems, it is possible for users with permission to modify certain AD attributes to impersonate privileged users and gain access to unauthorized resources on domain-joined Linux hosts.

To avoid problems relating to this vulnerability, SUSE has enabled the Kerberos local authentication plugin by default in `/etc/krb5.conf.d` and explicitly disabled the insecure Kerberos `auth_to_local` (`an2ln`) module:

```
[plugins]
         localauth = {
            disable = an2ln
            module = sssd:/usr/lib64/sssd/modules/sssd_krb5_localauth_plugin.so
}
```

Solution

Even with the adjustment made to `/etc/krb5.conf.d`, system updates will not automatically patch vulnerable systems where `/etc/krb5.conf` was modified to disable the use of the plugin. To ensure protection against attacks targeting this vulnerability, confirm that the Kerberos local authentication plugin is also properly enabled in the `/etc/krb5.conf file`.

Reference

- https://nvd.nist.gov/vuln/detail/CVE-2025-11561
- https://www.suse.com/security/cve/CVE-2025-11561.html

2.6 Training Solo aka CVE-2024-28956, CVE-2025-24495

Overview

Security researchers from the VUSec group at VU Amsterdam found a new Spectre v2 transient execution attack in Intel CPUs. The research focused on training the predictor within the same privilege class as the data to be leaked.

Three self-training attack classes were found:

- History-based attacks:
  Training can be performed using in-kernel methods, specifically classic Berkeley Packet Filter (cBPF) programs injected by the attacker. These programs are allowed for all users and are used for seccomp or packet filtering.
  Mitigations require additional code changes to the kernel; additionally, Intel implemented a new Indirect Branch History Fence (IBHF) instruction supplied by newer Intel CPU microcode (revisions 20250512 or newer).

- IP-based attacks:
  Attackers can force the prediction to fall back entirely on the branch address rather than history. That way, two indirect branches could train each other when their address aliases collide in the Branch Target Buffer. Usable gadgets to exploit this could be found—for example, within the Linux kernel—by using automated techniques.
  No mitigation is currently suggested.

- Direct-to-indirect attacks:
  On certain CPUs, direct branches can train indirect branch prediction. This behavior is caused by two hardware issues: Indirect Target Selection (ITS) (CVE-2024-28956) and a hardware issue on Lion Cove (CVE-2025-24495). For ITS, this drastically increases the self-training attack surface.
  Mitigations require Intel CPU microcode updates (revision 20250512 or newer) to supplement the Indirect Branch Predictor Barrier (IBPB) mitigation.
  Source code adaptations are also needed to add indirect jumps in the upper levels of the cache line, which mitigates the problem.

Solution

SUSE has released updated `ucode-intel` packages. CVE-2025-24495 is entirely mitigated by the `ucode-intel` update and does not require kernel changes. In contrast, the CVE-2024-28956 mitigation requires both Intel CPU microcode updates and kernel changes.

A new reporting file is added:`/sys/devices/system/cpu/vulnerabilities/indirect_target_selection`.

It can have the following content:

- Vulnerable

The kernel is vulnerable to the Indirect Target Selection attack.

- Mitigation: Aligned branch/return thunks
  The attack is mitigated in the kernel by aligned branch and return thunks.

- Mitigation: Retpolines, Stuffing RSB
  The attack is mitigated in the kernel by retpolines and/or RSB stuffing.

Configuration:

- indirect_target_selection = on
  The mitigations for Indirect Target selections are enabled if needed.

- indirect_target_selection = off
  The mitigations for Indirect Target selections are disabled.

- indirect_target_selection = force
  The mitigations for Indirect Target selections are always enabled.

If not specified, this mitigation follows the global “mitigations” command line setting.

Reference

- https://www.vusec.net/projects/training-solo/
- https://www.suse.com/security/cve/CVE-2024-28956
- https://www.suse.com/security/cve/CVE-2025-24495
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01153.html

3 Vulnerability management in 2025

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 aligns with standard security best practices or whether there are major vulnerabilities—such as buffer overflows or unintended privilege escalation—or security gaps

within potential attack vectors. 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. We continued to see an increased number of kernel security vulnerabilities being reported and fixed. The introduction of new AI-based tools has contributed to this rise, while simultaneously improving the quality of these reports over time.

TABLE 1: VULNERABILITIES WITH A UNIQUE CVE IDENTIFIED, IMPACTING SUSE PRODUCTS IN 2025

Low	Moderate	Important	Critical
146	3645	753	37

TABLE 2: SECURITY UPDATES AND PATCHES RELEASED TO FIX THESE VULNERABILITIES IN 2025

Low	Moderate	Important	Critical
316	1633	2855	197

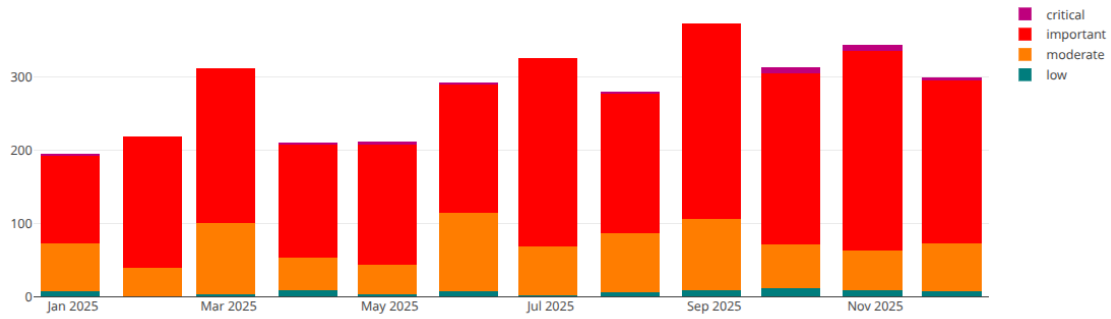

FIGURE 1: SECURITY UPDATES AND PATCHES RELEASED PER MONTH IN 2025

3.1 Continuous increase in the volume of reported kernel security vulnerabilities

In 2025, we continued to observe a high volume of security vulnerabilities reported to the National Vulnerability Database (NVD). The primary factor behind this statistical jump was the Linux kernel team's decision to become a CVE Numbering Authority (CNA) in 2024. Previously, the kernel relied on third parties to assign CVEs; now, the Linux team issues identifiers for nearly every security-related fix, including minor bugs that previously would have gone unreported. The kernel CNA's issuance criteria are broad, covering all use cases—from tiny embedded de-

vices to long-running enterprise systems—and cautiously flagging any bugfix that could potentially pose a security risk. As a result, the kernel CNA is issuing a massive number of CVEs that do not affect SUSE Linux product usage scenarios. This trend persisted throughout 2025, with our SUSE Product Security team processing more than 11,000 kernel CVEs over the last two years.

3.2 Record volume of security vulnerabilities discovered and remediated

Last year, we observed a 35% increase in security vulnerabilities impacting one or more SUSE or openSUSE products. However, this surge does not necessarily indicate that the systems have become less secure; rather, it reflects fundamental shifts in how bugs are discovered and documented. Furthermore, the widespread adoption of AI tools has shifted the balance between detection and protection. Researchers are now leveraging large language models to simulate complex scenarios—such as parallel execution bugs—that traditional scanners often overlook. A notable example is CVE-2025-37899, a vulnerability in the kernel's SMB server discovered through AI-driven analysis.

Additionally, with more than half of organizations worldwide now using AI assistants to write code, the pace of software development has accelerated. This speed, however, often introduces new vulnerabilities when sufficient security controls over AI-generated code are lacking. Given Linux's dominance in cloud environments, containers, and IoT devices, it remains a primary target for sophisticated threat actors, leading to unprecedented scrutiny of the system by malicious entities.

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/).

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.

In February 2023, SUSE began generating CSAF data for its security update notices and CVEs, including a complete back catalog of all historical 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 comprehensive yet straightforward JSON structure, allowing for seamless integration into other tools, even without the need for additional libraries.

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

OSV is an open source vulnerability database and triage infrastructure initiated by Google to assist both maintainers and consumers of open source software. SUSE provides regularly updated OSV data, which can be accessed at https://ftp.suse.com/pub/projects/security/osv/.

5 Commitment to the highest level of trust and reliability

January 24th 2025

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) technical requirements, and under the IPv6 Ready Logo Program (https://www.ipv6ready.org/db/index.php/public/logo/02-C-002792/).

January 24th 2025

SUSE Linux Enterprise Micro 5.3 has attained Common Criteria (CC) Certification. It is the first-ever product security certification for SLE Micro and documents compliance with the CC standard for the NIAP General Purpose Operation System (GPOS) protection profile. More information can be found at https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/CC/Betriebssysteme/1214.html and https://www.suse.com/support/security/certifications/. This certification is frequently mandatory for customers in highly regulated sectors, such as financial services, healthcare, pharmaceuticals, and the public sector.

February 6th 2025

SUSE has attained Service Organization Control (SOC) 2 and SOC 3 information security certifications for both SUSE Corporate and Rancher Prime Hosted. The SOC 2 (Service Organization Control) Type 2 reports provide a comprehensive assessment of SUSE's organizational security controls over the one-year audit period. These reports demonstrate to our clients and partners that their data is protected effectively and consistently. This achievement builds trust by proving that SUSE maintains a defined set of security practices and operates them effectively. Such certifications are essential for securing business deals, particularly with large enterprises that demand high data security standards. They also help in mitigating risks and identifying potential gaps that may require updated policies or procedures. SOC 2 reports are shared on a need-to-know basis and can be provided to clients upon request, while SOC 3 reports are available publicly online.

February 7th 2025

NIST has updated their site outlining the process for handling updates, patches, and CVEs for certified modules. Find their statement at https://csrc.nist.gov/Projects/cryptographic-module-validation-program/cmvp-flow under the section entitled "FIPS Validation and Updates, Patches, and CVEs".

March 6th 2025

SUSE has transitioned to a new certificate authority, LRQA Group Limited, and successfully completed certification for the new versions of ISO 27001:2022 and ISO 27701:2019. These 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. To request the latest certificate, contact: `cybersecurity@suse.com`.

November 1st 2025

SUSE has successfully renewed its ISO 27001:2022 and ISO 27701:2019 certifications through LRQA. These certifications reaffirm SUSE's continued commitment to information security and privacy excellence. This achievement demonstrates that SUSE's Information Security Management System (ISMS) and Privacy Information Management System (PIMS) meet internationally recognized standards, providing our customers, partners, and employees with confidence that data is managed securely and responsibly. You can download the renewed certifications via the link ISO 27001 (https://www.suse.com/support/security/certifications/SUSE-ISO-27001-ISO-27701.pdf) or ISO 27701 (https://www.ipv6ready.org/db/index.php/public/logo/02-C-002792/).

November 26th 2025

SUSE has attained NIST FIPS 140-3 certification for SUSE Linux Enterprise Server (SLES) 15 SP6 OpenSSL 3 Cryptographic Module.

6 About SUSE

SUSE is a global leader in enterprise open source software, across Linux operating systems, Kubernetes container management, Edge solutions and AI. The majority of the Fortune 500 rely on SUSE to provide resilient infrastructure, enabling IT leaders to optimize cost and manage heterogeneous environments. SUSE collaborates with partners and communities to provide organizations with choices to maximize their current IT systems and innovate with next-generation technologies across traditional on-premises, to cloud native, multi-cloud to edge and beyond. 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 pandemics 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

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 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.