SUSE Best Practices

Security

SUSE Solution Security Risk Report 2021

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 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 objective of this report is to provide a summary of all security vulnerabilities which affected SUSE products in calendar year 2021.

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

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. This implies to

- 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.

At the same time, any software can also contain errors (both deliberate and accidental) which could affect the system's security, including design flaws, programming errors, and backdoors.

The SUSE Security Team addresses all of these 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 such an excellent reputation for security.

2 Background

Software provides security features (such as authentication methods, encryption, intrusion prevention and detection, backup and others). However, it can also contain errors (such as design flaws, programming errors, and even backdoors) that often turn out to be relevant for the system's security. The SUSE Security Team's task is to addresses all of these aspects of software security, with the understanding that security in software is a challenge that never ends. Software security cannot be understood a state taken at some certain point in time; it is a process that must be filled with professional expertise and permanent development, both on software and on skills. The resulting evolution is what has given open source software, Linux and SUSE its excellent reputation for security.

A modern Linux operating system, such as SUSE Linux Enterprise Server for enterprise use or the openSUSE community distribution for home use, features a rich set of security programs and functions that range from access controls, intrusion prevention and detection, flexible and trustworthy authentication mechanisms, encryption for files and network connections, file integrity checking utilities, to network analysis tools and monitoring/logging utilities for your system. To complement this, there are advanced tools that help you to securely configure and administer your system, and to securely download and install update packages. These utilities are standard in SUSE products. The update packages fix security bugs that have been found after your product has been released. The security features of your Linux system are waiting for you to explore them. SUSE encourages our customers to take advantage of them to further improve the level of privacy and security that is built into every system by default.

Programs are usually written by humans, and humans make mistakes. By consequence, all software can contain errors. Some of these errors appear as instabilities (the software or the entire system crashes), while others may not have any apparent, visible effect. However, some software errors may introduce a security risk. A local or a remote attacker may be able to feed specially drafted data to the software which takes advantage of the programming error (in the case of a remotely exploitable bug, the data comes from an attached network device, such as a cable or DSL modem, or a wireless network interface card). The application then either crashes, resulting in a Denial of Service (DoS) attack, or it executes code that originates from the attacker, transferring control over the execution context from what the programmer intended to what the attacker has in mind for the exploitation of the error. Depending on the software's function, the resulting security breach can impose little or high security risks for your data and your system, potentially giving an attacker the opportunity to delete, alter or even steal your data, or use the system for his own purposes.

The SUSE Solution Security team is responsible for handling all SUSE product-related security incidents. In that team, clear and well-defined roles are assigned for tracking new incidents and coordinating needed updates. The team works with all SUSE engineering software specialists.

We use multiple sources to understand security incidents. These sources include the Mitre and NVD Common Vulnerabilities and Exposures (CVE) databases, various security mailing lists (OSS security, Linux distros, distros, bugtraq, and full-disclosure), direct reports, and other Linux vendors databases. We are also part of various pre-notification mailing lists for software components, like Xen, Samba, X.ORG. Confidential pre-notifications about vulnerabilities will be treated according to established responsible disclosure procedures.

3 Incident rating and tracking

We rate the severity of incidents with two different systems, a simplified rating system and the Common Vulnerability Scoring System (CVSS) v3.1 scoring system. The CVSS is an open framework for communicating the characteristics and severity of software vulnerabilities. It is being developed by the US-based non-profit organization FIRST.org: Its main goal is to assign the right score to a vulnerability to help security administrators prioritize responses and resources to specific threats. CVSS v3.1 scoring consists of three metric groups: Base, Temporal, and Environmental. The Base group represents the intrinsic qualities of a vulnerability that are constant over time and across user environments. The Temporal group reflects the characteristics of a vulnerability that change over time. The Environmental group represents the characteristics of a vulnerability that are unique to a user's environment. The Base metrics produce a score ranging from 0 to 10, which can then be modified by scoring the Temporal and Environmental metrics. A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score. Today, SUSE uses the Base score methodology to evaluate vulnerabilities throughout the support lifecycle of our products. SUSE keeps the right to adjust the final score of the vulnerability as more details become known and available throughout the analysis. The most current CVSS resources can be found at https://www.first.org/cvss/ . The CVSS v3.1 calculator used by SUSE could be found at https://www.first.org/cvss/calculator/3.1. The framework is measuring the severity of a given vulnerability, not the associated risk alone. The scoring of any vulnerability may vary with different analysts hence the final score could be slightly different between vendors impacted by that vulnerability. For a more accurate assessment of the impact, vendors and application owners must always consider factors outside of CVSS such as exposure or threat.

The security incidents are tracked in our own workflow system, technical details are tracked in the SUSE bug-tracking system, and the updated software package is built, processed, and published by our internal “Open Build System”. Internal Service Level Agreements (SLAs) corresponding to the severity rating are monitored and reviewed regularly. Our packagers backport the required security fixes to our version of the software. To protect the stability of our customer setups, we only rarely do minor version upgrades. After receiving fixes for the affected software, four eye reviews cross-check the source patches. A number of automated checks verify source and binary compatibility and the completeness of patch meta information. They also check whether patches can be installed without problems. Dedicated QA teams provide integration, bugfix, and regression testing for all updates before they are released to our customers.

After the release of an update, automated processes publish the updates, update notices, and cross reference information on our CVE index pages and machine-readable OVAL and CVRF XML information.

The objective of this report is to provide a summary of all security vulnerabilities which affected SUSE products in calendar year 2021. We will go into details on the high impact vulnerabilities which affected our products in 2021 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:

TABLE 1: INCIDENT RATING AND CVSS SCORE

Rating	CVSS Score	Definition
Critical	9.0 and above	This rating is given to flaws that could be easily exploited by a remote unauthenticated attacker and lead to system compromise (arbitrary code execution) without requiring user interaction. These are the types of vulnerabilities that can be exploited by worms. Flaws that require an authenticated remote user, a local user, or an unlikely configuration are not classed as critical impact.
Important	7.0 to 8.9	This rating is given to flaws that can easily compromise the confidentiality, integrity, or availability of resources. These are the types of vulnerabilities that allow local users to gain privileges, allow unauthenticated remote users to view resources that should otherwise be protected by authentication, allow authenticated remote users to execute arbitrary code, or allow remote unauthenticated users to cause a denial of service without user interaction.
Moderate	4.0 to 6.9	This rating is given to flaws that may be more difficult to Copyright © SUSE 2022 5 exploit but could still lead to some compromise of the confidentiality, integrity, or availability of resources, under certain circumstances. These are the types of vulnerabilities that could have had a critical impact or important impact but are less easily exploited based on a technical evaluation of the flaw, or affect unlikely configurations. Local, persistent (service needs to be restarted) denial of service conditions for basic system services (kernel,

Rating	CVSS Score	Definition
		systemd, polkit, dbus, etc.) with and without user interaction should also be rated “moderate”.
Low	up to 3.9	This rating is given to all other issues that have a security impact. These are the types of vulnerabilities that are believed to require unlikely circumstances to be able to be exploited, or where a successful exploit would give minimal consequences.

4 When to prefer version upgrades over backports

It is a general policy rule that no new upstream versions of a package are introduced into our enterprise products. This rule is not an absolute rule however. For certain types of packages, in particular antivirus software, security concerns weigh heavier than the conservative approach that is preferable from the perspective of quality assurance. For packages in that class, occasionally newer versions are introduced to a released version of an enterprise product line.

Sometimes also for other types of packages the choice is made to introduce a new version rather than a backport. This is done when producing a backport is not economically feasible or when there is a very relevant technical reason to introduce the newer version.

5 Major security vulnerabilities in 2021

5.1 Log4Shell

Overview

On Friday, December 10th 2021, a new vulnerability in the “log4j” Java logging framework was reported, which could be trivially exploited. The 0-day exploit in the log4j Java logging framework was found by Chen Zhaojun of Alibaba Cloud Security Team, which allowed remote attackers able to inject strings into log4j based Java logging to execute code by exploiting the default enabled JNDI bindings. This is possible without any preconditions, making it critical. This vulnerability is caused by a new feature introduced in log4j 2.x versions where a specific string embedded in messages logged by log4j would be interpreted as Java code.

The vulnerability, also called "log4shell" does not impact SUSE Linux Enterprise products directly as these are still shipping an older version of log4j that is not affected by this bug.

SUSE Rancher is not affected by this vulnerability. The Helm chart for Istio 1.5, provided by Rancher and which is currently deprecated, includes Zipkin and is vulnerable to log4j. Customers are advised to upgrade to the recent Istio version provided in Cluster Explorer, which does not uses Zipkin and is not affect to the vulnerability.

The vulnerability does not affect SUSE Manager, as it is using at most log4j 1.2.x, which is not affected. One component of SUSE OpenStack Cloud ("storm") embeds log4j 2.x, which immediately received the required update. The SUSE NeuVector product is not affected by this vulnerability, but its security scanner functionality has now added support for scanning your containers, see the NeuVector log4j2 page.

A much less severe similar vulnerability was discovered in older log4j 1.2.x versions via the JMS interface. This JMS functionality is not default enabled, administrators must have enabled it. SUSE has also published updates for log4j 1.2 versions disabling the JMS functionality completely.

For the log4j 1.2.x packages, SUSE is already fixing security issues in these packages, even though upstream has declared them end-of-life. In parallel, SUSE will ship log4j 2.x versions where possible so customers can migrate to the newer log4j major release.

Solution

SUSE considers log4j versions 2.0 and newer as affected, log4j 1.2.x does not have the same critical vulnerability and is not considered affected by this CVE.

- SUSE OpenStack Cloud embeds log4j2 in the "storm" component, which received updates within 5 days of the initial vulnerability announcement. SUSE customers are advised to get the release security update for the mitigation of this vulnerability.
- SUSE Linux Enterprise products do not ship log4j 2.x.
- SUSE Manager does not ship log4j 2.x.
- SUSE Enterprise Storage does not ship log4j 2.x.
- SUSE NeuVector product does not ship log4j 2.x

References

- SUSE CVE Web page for CVE-2021-44228: https://www.suse.com/security/cve/CVE-2021-44228.html
- SUSE CVE Web page for CVE-2021-45046: https://www.suse.com/security/cve/CVE-2021-45046.html
- SUSE CVE Web page for CVE-2021-4104 (log4j 1.2): https://www.suse.com/security/cve/CVE-2021-4104.html
- log4j security apara>log4j security advisory: https://logging.apache.org/log4j/2.x/security.html
- SUSE Technical Information Document (TID) 000020526: https://www.suse.com/support/kb/doc/?id=000020526
- NeuVector article about *log4j2* scanning addition: https://blog.neuvector.com/article/apache-log4j-2-cve-2021-44228
- US CISA guidance for *log4j2*: https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance
- BSI notification about *log4j2* (PDF): https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2021/2021-549032-10F2.pdf?__blob=publicationFile&v=3

5.2 SADDNS / Dnspooq

Security researchers from University of California and Tsinghua University have identified a new variant of DNS cache poisoning attacks called SADDNS ("Side-channel AttackeD DNS") due to a side channel attack against ICMP replies.

As DNS is primarily UDP-based, it is open to malicious package injection attacks, and various have been identified over time. The DNSSSEC enhancement would fix the package injection attacks using cryptographic integrity protection, but is not yet widely deployed.

When using traditional DNS, there have been two primary mitigations against this kind of poisoning been added:

- Randomization of the transaction ID (a 16 bit identity in every DNS packet)
- Randomization of the UDP port sending/receiving the replies (another 16 bit entity)

The researchers have now shown that the current Linux kernels have a side-channel attack using predictable ICMP port-unreachable replies on non-open UDP ports, like for example DNS reply ports, which allows attackers to remotely detect the open ports.

Making it a 32-bit wide space to exhaust for brute force attacks would also reduce the attack surface to 16 bit space, making DNS cache poisoning attacks again possible.

Solution

The best solution is to remove this side channel attack from the Linux kernel. The reappearance of the DNS cache poisoning attack allows remote attackers to pretend to be different hosts if your host is reachable from the Internet, allowing man-in-the-middle attacks against encrypted communication or software delivery.

SUSE is delivering Linux kernel updates to again mitigate the SADDNS attack. We also recommend to use DNSSEC, which in general avoids this kind of attack.

SADDNS, while potentially serious to not patched systems, poses little danger to those who keep their SUSE product patched and up to date. SUSE released fixes and updates to all affected versions, eliminating the potential for disruption.

References

- SAD DNS Web site: https://www.saddns.net/ ↗
- SUSE TID 19786: https://www.suse.com/support/kb/doc/?id=000019786 ↗
- SUSE CVE-2020-25705 Web page: https://www.suse.com/security/cve/CVE-2020-25705/ ↗

5.3 Baron Samedit: Heap-based buffer overflow in `sudo`

Security researchers from Qualys discovered a new vulnerability in `sudo` which allows unauthenticated attackers to gain root privileges. The attackers need to have access to the system as a user to exploit this vulnerability but after they are logged in they do not need to provide any further authentication password to escalate their privilege to root.

The vulnerable code that causes the heap-based buffer overflow was introduced in `sudo` version 1.8.2.

- SUSE Linux Enterprise Server 12 and SUSE Linux Enterprise Server 15 products are affected.
- SUSE Linux Enterprise Server 11 products are not affected.

Solution

Fixes have been provided for all affected and supported SUSE products. For more details, check the CVE Web page referenced below.

References

- Bug report: https://bugzilla.suse.com/show_bug.cgi?id=1181090
- SUSE CVE-2021-3156 Web page: https://www.suse.com/security/cve/CVE-2021-3156/
- Qualys Security Advisory article: https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-based-overflow-sudo.txt

5.4 Salt: Several remote code execution vulnerabilities

SaltStack announced a security release fixing several critical issues. The issues range from privilege escalation, missing TLS/SSL certificate validation, or directory traversal to possible command injection.

Solution

SUSE released fixes and updates for all of the affected and supported SUSE products. See the CVEs referenced below:

- CVE-2020-28243: A privilege escalation is possible on a SaltStack minion when an unprivileged user can create files in any non-blacklisted directory via a command injection in a processes' name. Simply ending a file with “(deleted)” and keeping a file handle open to it is enough to trigger the exploit whenever a restart check is triggered from a SaltStack master.
- CVE-2020-28972: In SaltStack Salt v2015.8.0 through v3002.2, authentication to vCenter, vSphere, and ESXi servers does not always validate the TLS/SSL certificate.

- CVE-2021-3148: This is an issue in SaltStack Salt v2016.3.0 through v3002.2. Sending crafted Web requests to the Salt API, when using the SSH client, can result in command injection.
- CVE-2021-25281: The Salt API does not honor *eAuth* credentials for the wheel_async client. Thus, an attacker can remotely run any wheel modules on the master.
- CVE-2021-25282: The *salt.wheel.pillar_roots.write* method is vulnerable to directory traversal.
- CVE-2021-25283: The *jinja* render does not protect against server-side template injection attacks.
- CVE-2021-3144: *eAuth* tokens can be used once after expiration.
- CVE-2021-25284: *Salt.modules.cmdmod* can log credential to the “error” log level
- CVE-2021-3197: The Salt-API's SSH client is vulnerable to a shell injection by including *ProxyCommand* in an argument, or via *ssh_options* provided in an API request.
- CVE-2020-35662: In SaltStack Salt v2015.8.0 through v3002.2, when authenticating to services using certain modules (*asam runner, qingcloud, splunk returner, panos proxy, cimc proxy, zenoss module, esxi module, vsphere module, glassfish module, bigip module, and keystone module*), the SSL certificate is not always validated.

5.5 OMIGOD

Security researchers found that Microsoft Azure injects a specific health monitoring package “OMI agent” into public cloud Linux instances when certain other Azure services are enabled for a given instance.

The services known to trigger the injection of the vulnerable package are as follows:

- Azure Automation
- Azure Automatic Update
- Azure Operations Management Suite (OMS)
- Azure Log Analytics
- Azure Configuration Management
- Azure Diagnostics

The deployed code has several easy-to-exploit remote vulnerabilities. See the CVEs listed below:

- CVE-2021-38647: Unauthenticated RCE as root (Severity: 9.8)
- CVE-2021-38648: Privilege Escalation vulnerability (Severity: 7.8)
- CVE-2021-38645: Privilege Escalation vulnerability (Severity: 7.8)
- CVE-2021-38649: Privilege Escalation vulnerability (Severity: 7.0)

To see if your instance is using the code in question, use:

```
rpm -qa omi
```

As the package is maintained and injected by Microsoft into Azure instances, and is not delivered by SUSE, SUSE cannot provide fixes.

Solution

Visit https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38647 ↗ for more details on this vulnerability. You should take several steps to prevent your IT environment from being vulnerable to the OMIGOD vulnerability:

- Verify your network settings and ensure ports 5985, 5986, 1270 are not exposed to the Internet. If these ports are exposed to the Internet, it is recommended to consider your system as compromised.
- Redeploy your instance using a network construct with ports 5985, 5986, 1270 closed to the Internet.

If this is not feasible, follow the installation steps for SUSE at https://docs.microsoft.com/en-us/windows-server/administration/Linux-Package-Repository-for-Microsoft-Software ↗ :

- SUSE Linux Enterprise Server 12: `sudo rpm -Uvh https://packages.microsoft.com/config/sles/12/packagesmicrosoft-prod.rpm`
- SUSE Linux Enterprise Server 15: `sudo rpm -Uvh https://packages.microsoft.com/config/sles/15/packagesmicrosoft-prod.rpm`
- Run `zypper up` to update the omi agents from the newly added repo.

5.6 DHEATER

Security researchers from Balasys have published a new attack on Diffie-Hellman key exchange which allows remote attackers to attack network facing SSL / TLS / HTTPS / SSH services. This is leading to excessive compute time usage already by sending small amounts of network traffic even before authentication. All applications on SUSE Linux Enterprise that have DHE enabled are affected. The Diffie-Hellman Epheremal key exchange is usually configured by default to provide perfect forward secrecy. The Elliptic Curve Diffie-Hellman protocol is not affected by this vulnerability.

Solution

This vulnerability is a protocol level problem. SUSE continues to monitor if and when cryptographic libraries will develop and implement counter measures in their DiffieHellman code, and then backport those fixes. Up to then, the DHE key exchange method should be disabled and the Elliptic Curve Diffie-Hellman method should being used as a workaround.

SUSE recommends to disable the DHE key exchange until a technological solution is found, using methods listed in the “additional information” section. While we use *DEFAULT_SUSE* as a default cipher set, removing DHE unconditionally could break existing setups. Thus SUSE will not remove it proactively at this time.

A workaround is to temporary disable DHE key exchange and only use ECDHE (Elliptic Curve Diffie-Hellman) in SSL / TLS / HTTPS using network services. System administrators should check first if this causes interoperability issues.

References

- GitHub repository: https://github.com/Balasys/dheater ↗
- SUSE CVE-2002-20001 Web page: https://www.suse.com/security/cve/CVE-2002-20001.html ↗

5.7 boothole-2: GRUB2 UEFI secure boot bypass issues

Various security researchers and the GRUB2 team have published more security issues in GRUB2, which can be used to bypass UEFI segrubcure boot chain. These security issues have the same scope as the BootHole issues from 2020.

This attack requires root access to the boot loader used in Linux operating systems, GRUB2. It bypasses normal Secure Boot protections to persistently install malicious code which cannot be detected by the operating system. Given the need for root access to the boot loader, the described attack appears to have limited relevance for most cloud computing, data center and personal device scenarios, unless these systems are already compromised by another known attack. However, it does create an exposure when untrusted users can access a machine, for example bad actors in classified computing scenarios or computers in public spaces operating in unattended kiosk mode. These are scenarios which Secure Boot was intended to protect against.

Solution

Software and hardware vendors are closely collaborating to ensure that sophisticated attackers cannot reinstall old versions of GRUB2. Over time, vendors are going to update cryptographic keys in the BIOS for new computers, and to provide so-called DBX Exclusion List updates for existing computers. These can prevent systems that are not patched and old installation media from starting. Make sure you have installed all relevant boot loader and operating system updates for BootHole before installing a BIOS or DBX Exclusion List update to ensure continuity.

SUSE has released fixed GRUB2 packages which close the vulnerabilities for all of SUSE's Linux-based products. SUSE has also released the corresponding Linux kernel packages, cloud image and installation media updates.

References

- Blog article: https://www.suse.com/c/suse-addresses-another-grub2-uefi-secure-boot-security-exposure/ ↗

5.8 Sequoia (kernel root exploit in fs layer)

Security researchers from Qualys have identified a security issue in the Linux Kernel where local attackers could reliably exploit an integer overflow to execute code in the kernel and so escalate privileges. *fs/seq_file.c* in the Linux kernel 3.16 through 5.13.x before 5.13.4 does not properly restrict seq buffer allocations, leading to an integer overflow, an *Out-of-bounds Write*, and escalation to root by an unprivileged user, aka CID-8cae8cd89f05.

Qualys refers to this vulnerability as “Sequoia: A deep root in Linux's filesystem layer (CVE2021-33909)”.

Solution

SUSE advises all customers to update to the latest released kernel after July 20, 2021.

References

- SUSE CVE 2021-33909 Web page: https://suse.com/security/cve/CVE-2021-33909.html
- Qualys Security Advisory article: https://www.qualys.com/2021/07/20/cve-2021-33909/sequoia-local-privilege-escalation-linux.txt

5.9 FRAGATTACKS - several WLAN vulnerabilities

Security Researcher Mathy Vanhoef discovered various attacks against Wi-Fi (802.11) stacks and against the Wi-Fi standard related to Wi-Fi fragments. This vulnerability is documented on the Web site https://www.fragattacks.com/ and is called FRAGATTACKS.

This set of vulnerabilities can allow local attackers in Wi-Fi range to inject traffic even in encrypted Wi-Fi networks, or get access to information of other users in the same Wi-Fi network. If the system is not using Wi-Fi, it is not affected. These issues largely affect the hardware / firmware of Wi-Fi cards.

Two CVEs are also included in the mac80211 stack of Linux, and will be addressed by updates to the Linux kernel. These issues have received CVE-2020-24586 and CVE-2020-24587. These and others CVEs are fixed in the various Wi-Fi firmware. We will release the respective updates when they become available from the Wi-Fi card vendors Linux support, via “kernel-firmware” updates.

Solution

SUSE advises all customers to install the published updates required to fix the following vulnerabilities:

- CVE-2020-24586: Fragmentation cache not cleared on reconnection
- CVE-2020-24587: Reassembling fragments encrypted under different keys
- CVE-2020-24588: Accepting non-SPP A-MSDU frames, which leads to payload being parsed as an L2 frame under an A-MSDU bit toggling attack

- CVE-2020-26139: Forwarding EAPOL from unauthenticated sender
- CVE-2020-26140: Accepting plaintext data frames in protected networks
- CVE-2020-26141: Not verifying TKIP MIC of fragmented frames
- CVE-2020-26142: Processing fragmented frames as full frames
- CVE-2020-26143: Accepting fragmented plaintext frames in protected networks
- CVE-2020-26144: Always accepting unencrypted A-MSDU frames that start with RFC1042 header with EAPOL ethertype
- CVE-2020-26145: Accepting plaintext broadcast fragments as full frames
- CVE-2020-26146: Reassembling encrypted fragments with non-consecutive packet numbers
- CVE-2020-26147: Reassembling mixed encrypted/plaintext fragments

6 Vulnerability Management in 2021

The SUSE Solution Security team observed a steady amount of vulnerabilities hitting our products on an annual basis. More and improved tools are now available for finding out zero-day vulnerabilities and scanning for existing vulnerabilities. Such instruments can validate and report back if the application code written is following the standard security best practices or there are major gaps in potential attack vectors such as buffer overflow, denial of service or unwanted elevated access. It is obvious that developers are becoming more and more security aware and the quality of the code being developed has greatly improved in both quantity and quality. While we notice an increasing number of important vulnerabilities, the number of critical vulnerabilities is going down year over year.

TABLE 2: VULNERABILITIES WITH A UNIQUE CVE IDENTIFIED, IMPACTING SUSE PRODUCTS

Year	Moderate	Important	Critical
2021	781	591	48
2020	830	560	48
2019	1003	495	55

TABLE 3: SECURITY UPDATES AND PATCHES RELEASED TO FIX THESE VULNERABILITIES

Year	Moderate	Important	Critical
2021	401	887	68
2020	402	775	80
2019	432	558	77

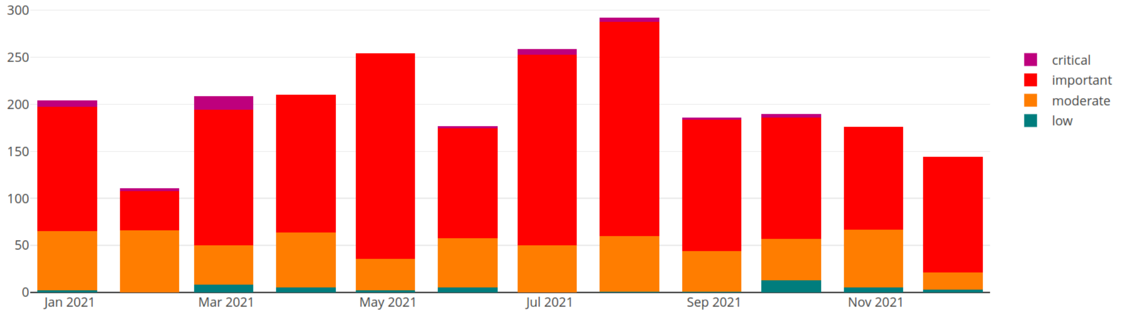

FIGURE 1: SECURITY UPDATES AND PATCHES RELEASED PER MONTH

Key Performance Indicators

- 100 percent of all high impact vulnerabilities had an update or a patch released to our customers within five business days.
- 97 percent of all vulnerabilities scored CVSS 4.0 and above had an update or a patch released to our customers within 180 calendar days.
- 88 percent of all vulnerabilities scored CVSS 4.0 and above had an update or a patch released to our customers within 90 calendar days.

7 Secure Software Supply Chain

Securing our software supply chain is a top priority for SUSE to ensure that our customers are protected from security risks, known and zero-day vulnerabilities. Ensuring that no threat actor can inject malicious code within our build service systems is certified by industry leading security certifications. Our teams continually work to certify all SUSE products, and develop security solutions to ensure the highest level of trust and reliability for our customers.

Common Criteria (CC), also known as the Common Criteria for Information Technology Security Evaluation, is an international set of specifications and guidelines designed by the signatories of the Common Criteria Recognition Arrangement (CCRA), to evaluate information security products and systems. It was developed to ensure that products and systems meet a predefined security standard for government deployments. Products and systems that have been successfully tested and evaluated by a licensed laboratory are awarded a Common Criteria certification. On November 11th 2021, SUSE was awarded with the Common Criteria Certification (NIAP OSPP) for SUSE Linux Enterprise Server 15 SP2. This certification is mandatory for work with the United States (US) Federal Government. It demonstrates compliance to NIAP Protection Profile for General Purpose Operating Systems, Version 4.2.1 (CCEVS-VR-PP-0047) with the Extended Package for Secure Shell (SSH), Version 1.0 (CCES-VR-PP-0039). This certification extends our Common Criteria Certification track by US Compliance Regulations enabling US federal entities to profit from SUSE's Certified Secure Software Supply Chain while complying with all necessary national regulations.

The National Institute of Standards and Technology (NIST) developed the FIPS 140-2 security standard. It outlines the security requirements that must be satisfied by cryptographic modules, providing four increasing, qualitative levels intended to cover a wide range of potential applications and environments. On October 27th 2021, NIST awarded SUSE a validation certificate for the Libica Cryptographic Module, a software-hybrid module that provides general purpose cryptographic algorithms to applications running in the user space of the underlying operating system, SUSE Linux Enterprise Server on the IBM Z mainframes. More details about SUSE Linux Enterprise Server on IBM Z can be found at https://www.suse.com/products/systemz/ ↗.

Many other industry standards like Defense Counterintelligence Security Agency (DCSA) and the Defense Information Systems Agency (DISA) Security Requirements Guides (SRGs) and Security Technical Implementation Guides (STIG) depend on FIPS 140-2 certified cryptography modules. On July 22nd 2021, the National Institute of Standards and Technology (NIST) under the Cryptographic Module Validation Program (CMVP) in compliance with the Federal Information Processing Standards (FIPS) 140-2, has validated all modules within SUSE Linux Enterprise Server 15 SP2. More details can be found at https://documentation.suse.com/sles/15-SP3/html/SLES-all/cha-security-fips.html ↗ .

On July 8th, 2021, SUSE announced that SUSE Linux Enterprise Server 15 SP2 is now EAL 4+ level certified for IBM Z, Arm and x86-64. SUSE is the only provider of a recent general-purpose Linux operating system with a secure software supply chain that is certified Common Criteria EAL 4+ for all these platforms. SUSE Linux Enterprise Server 15 SP2 was certified by BSI, Germany's Federal Office for Information Security, based on an evaluation conducted by atsec information security. To achieve the certifications, the SUSE products, and processes for developing and maintaining its products, passed a rigorous security evaluation performed by Atsec Information Security. The certificates were issued by Bundesamt für Sicherheit in der Informationstechnik (BSI) the German Federal Office for IT Security. The Common Criteria for Information Technology Security Evaluation is an international standard (ISO/IEC 15408), recognized by 26 countries (CCRA) worldwide. Details regarding SUSE's full "Common Criteria Part 3 conformant EAL 4 augmented by ALC_FLR.3 Systematic Flaw Remediation" certification are listed at https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/CC/Betriebssysteme/1151.html?nn=513260 ↗ .

On January 29th 2021, the Defense Information Systems Agency (DISA) has released the SUSE Linux Enterprise Server 15 Security Technical Implementation Guide (STIG). Details regarding STIG can be found at https://www.suse.com/c/sles-15-security-technical-implementation-guide-stig/ ↗ .

8 About SUSE

SUSE is a global leader in innovative, reliable and enterprise-grade open source solutions, relied upon by more than 60% of the Fortune 500 to power their mission-critical workloads. We specialize in Enterprise Linux, Kubernetes Management, and Edge solutions, and collaborate with partners and communities to empower our customers to innovate everywhere – from the data center, to the cloud, to the edge and beyond. SUSE puts the "open" back in open source, giving customers the agility to tackle innovation challenges today and the freedom to evolve their strategy and solutions tomorrow. The company employs nearly 2000 people globally and is listed on the Frankfurt Stock Exchange. For more information, visit https://www.suse.com ↗.

9 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 and these views could change. SUSE 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 SUSE's views as of any date other than the publication date of this document.

10 Legal notice

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

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.