Business Paper

May 2022

SUSE Security Situation Advisory Guide (SUSE S^{2}UAG) v. 1.1

Securing and Hardening SUSE Software

The risk of cyber attacks is on the rise, and not only due to the war in Ukraine. An increasingly digitalized world can also lead to higher cyber vulnerability in organizations that do not incorporate security-oriented thinking and cybersecurity into their corporate cultures.

The ENISA counted 24 cases of supply chain attacks between January 2020 and June 2021 alone

(https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks). According to the Allianz Cyber Report, the first half of 2021 saw hacker attacks increase by 125 percent compared to the same period in 2020.

(https://www.tagesschau.de/wirtschaft/unternehmen/hackerangriffe-allianz-globalelieferketten-101.html).

Well-funded state actors are continually devising ever more deceptive attack tools that then proliferate into the world of crime. Cybercrime as a service, increasing awareness and securing supply chains are among the key cybersecurity trends in 2022. The protection of KRITIS is also a major topic.

The ever-increasing professionalization of cybercriminals should prompt medium-sized companies, industry and public authorities to implement fast and well-considered measures before an incident occurs.

What can SUSE customers and users do in the short term to improve system security?

The brief summary below is not exhaustive but provides an overview of possible immediate actions and approaches that can be taken with SUSE customer products. We recommend and assume that our customers have developed a security concept for their specific needs in relation to their use of SUSE products.

You can find references to further information as links in the text and in the overview at the end.

Keeping systems up-to-date

Inventory

One of the basic concepts of hardening systems is to have an overview of systems and services. This is the only way to identify and disable obsolete systems or services and to determine whether systems and services are still regularly supported and maintained with the latest updates.

When systems or services are no longer needed, they should be immediately decommissioned to reduce the attack surface.

Subscriptions

Are all systems registered and are the subscriptions still active?

Check the status of your systems via the SUSE Customer Center (https://scc.suse.com/) and/or SUSE Manager. On individual machines, "zypper lifecycle" can be used to check whether a SUSE product has reached the end of its life cycle.

Updates

Have all updates been installed/are all updates installed promptly?

- For individual systems, this can be checked using the command "zypper lp" and fixed using the command "zypper patch."
- If management systems such as SUSE Manager are used, the update status of these systems should be checked and improved in the long term through automation.
- If you work with maintenance windows, it is important to consider bringing forward scheduled windows with major and important updates rather than waiting weeks or months, as this will reduce the wait between maintenance windows.

Hardening Systems

Operating System Level

Hardening systems is a comprehensive action that must be carried out carefully so the hardening does not affect the intended usage scenarios. Always refer to our documentation (in English) https://documentation.suse.com/. These documents deal specifically with hardening operating system platforms:

Product	Link
SLES 12	Hardening Guide — SUSE Linux Enterprise Server 12 SP4 Hardening Guide | SUSE Linux Enterprise Server 12 SP5
SLES 15	Security and Hardening Guide | SUSE Linux Enterprise Server 15 SP1 Security and Hardening Guide | SUSE Linux Enterprise Server 15 SP2 Security and Hardening Guide | SUSE Linux Enterprise Server 15 SP3
SLES for SAP	Operating System Security Hardening Guide for SAP HANA for SUSE Linux Enterprise Server 15 GA and SP1

Application Protection

Another approach to protecting existing applications is to use

AppArmor. The AppArmor Framework provides a mandatory access control (MAC)

system that allows individual applications to grant access to required resources only while preventing unnecessary access. Existing services can continue to run without direct changes to the code, but their access to other system components is restricted by the operating system.

For more information about AppArmor, see the Security and Hardening Guide: **https:/documentation.suse.com/sles/15-SP3/html/SLES-all/chaapparmor-intro.html.**

Container and Kubernetes Environments Container Security:

NeuVector

Container environments orchestrated by Kubernetes quickly reach the limits of traditional hardware-based security concepts that use firewalls, routers and switches. The internal data traffic in the usual virtual networks there grows exponentially with the micro services used and, due to changing IP addresses and extremely fast container instantiation, it cannot be controlled with tools that do not know and understand the basic architecture. But it is precisely this that must be systematically and automatically monitored.

The NeuVector project enables network visibility, inspection and segmentation;

vulnerability, configuration and compliance management and risk profiling;

threat detection and incident response. NeuVector's open-source container images can be installed on any Kubernetes cluster and are available to cloud-native users of enterprise-container management platforms such as SUSE Rancher, Red Hat OpenShift, VMWare Tanzu, Google GKE, Amazon EKS and Microsoft Azure AKS. NeuVector is the first end-to-end open-source container security platform to provide zero-trust security for containerized workloads.

NeuVector's codebase has been available to the open-source community since January 2022 on

GitHub. https://neuvector.com/

Hardening: SUSE Rancher

SUSE Rancher capabilities are integrated with popular authentication tools and services and even offer role-based access control (RBAC) for Kubernetes infrastructures:

- Centralized user authentication enables local users to be set up and/or a connection to an external authentication provider to be established
- Built-in roles enable the configuration of user permissions for resources and the customization of the roles for each Kubernetes resource.

We recommend additional security scans to check whether Kubernetes is being run in accordance with the security requirements defined in the CIS Kubernetes Benchmark.

CVE: https://rancher.com/docs/rancher/v2.6/en/security/cve/

Hardening Guide: https://docs.rke2.io/

User Security

Many incident categories, such as phishing, credential stuffing or brute forcing, are the result of poorly secured user accounts.

One of the most successful methods of defense against this is to enable multi-factor authentication (MFA) for users. This must be set up differently in every environment, so general instructions cannot be provided here.

Hardening with Hardening Tools

SUSE has partnered with the American DISA to create a formal Hardening Guide (STIG) that can either be carried out manually or run automatically. The Hardening Guide is in a question-and-answer format that can be worked through with a specific tool and is well suited for audits.

This STIG is available on our website https://www.suse.com/support/security/certifications/ or can be downloaded from the DISA website, where you can also find STIGs for other products. For example, you can search for "SUSE" here: https://public.cyber.mil/stigs/downloads/.

The official tools for the application of a STIG can be downloaded here: https://public.cyber.mil/stigs/srg-stig-tools/.

SUSE also offers an automated variant—available in the "scap-securityguide" package—that was created from the ComplianceAsCode open-source project. This can be reviewed and adjusted automatically with "openscap."

Such automatic hardening cannot offer comprehensive protection and should be considered only one of several building blocks of an operational concept. Having an operational concept is also important for

striking the right balance between security and usability for the customer. Furthermore, it is advisable to embed it in an information security management (ISM) system. For more information, see the BSI's (*Bundesamt für Sicherheit in der Informationstechnik* — German Federal Office for Information Security) guide to basic protection: https://www.bsi.bund.de/DE/Themen/Unternehmen-undOrganisationen/Standards-und-Zertifizierung/IT-Grundschutz/itgrundschutz_node.html.

Proof of System and Supply Chain Security

The BSI awarded SUSE

Common Criteria Certification (EAL4+) in August 2021 for the SUSE Linux Enterprise Server 15

SP2. This certification is important for our customers because it documents and certifies SUSE's commitment to providing a secure software supply chain that has been developed to the highest government and industry standards, therefore providing our customers with the highest level of security. This standard verifies the security of the SUSE software supply chain for SLE 15 SP2 and awards it the government certificate. It is recognized in all signatory states of the CCRA and

SOG-IS MRA agreement. When drawing up tenders, please ensure that this proof of security is added to the requirements catalog.

In addition to the kernel, some libraries are also certified with the US standard FIPS 140-2 for the cryptography they provide. Their cryptographic capabilities and their behavior toward errors is therefore government verified.

A list of cryptographic modules can be found in the FIPS section on the

page https://www.suse.com/support/security/certifications/ SUSE

Security Information

Visit https://www.suse.com/security/ for security information related to SUSE products:

- SUSE update announcements: We recommend that managers and administrators subscribe to the appropriate mailing lists:
  - SUSE Linux Enterprise, SUSE Manager: https://lists.suse.com/mailman/listinfo/sle-security-updates
  - NeuVector: https://lists.suse.com/mailman/listinfo/neuvector-updates
- SUSE CVE pages: The affected or non-affected software is listed for each CVE
- Machine-readable data for SUSE updates in OVAL and CVRF format
- SUSE security ratings — describing both the basic rating and CVSS v3.1
- Handling security problems with SUSE (Flaw Remediation) • Security certification pages

* SUSE Linux Enterprise Server 15 SP2 has been certified by the BSI on the basis of an evaluation by atsec information security. More details on SUSE's certification "Common Criteria Part 3 conformant

EAL 4 augmented by ALC_FLR.3 Systematic Flaw Remediation" can be found on the pages of the BSI website: www.bsi.bund.de/SharedDocs/Zertifikate_CC/CC/Betriesystems/1151.html?nn=513260.

For more information about SUSE Linux Enterprise Server, visit https://www.suse.com/de-en/products/server/. For information on Common Criteria certification, visit www.commoncriteriaportal.org.

About SUSE

SUSE is a leading global provider of innovative, reliable, and secure open-source solutions for companies. Over 60 percent of the Fortune 500 rely on SUSE for their business-critical workloads. We specialize in business-critical Linux, enterprise container management, and Edge solutions and work with partners and communities to ensure that our customers have room for innovation — from the data center and the cloud to the Edge and beyond.

SUSE puts the "open" back into open source, giving customers the agility and innovation they need to overcome the challenges of today and the freedom to develop the strategy and solutions of tomorrow. SUSE has approximately 2000 employees worldwide and is listed on the Frankfurt Stock Exchange.

Find out more on www.suse.com.

SUSE is also an active member of the TeleTrusT Association, the BSI Alliance for Cybersecurity and the Zero Outage Alliance and is, of course, heavily involved in the open-source community.