

Patch it · Fix it · Run it

Patch me, if you can.

Flickst Du noch oder auditierst Du schon?

Christian Stankowic & Jörg Kastning

August 2026



Inhalt

- 1** Wer sind wir und warum sind wir hier?
- 2** Schwachstellen-Management
- 3** Patch-Management-Konzepte
- 4** Patch-Management-Werkzeuge
- 5** Q&A und Ausblick

Abschnitt

Wer sind wir und warum sind wir hier?

Jörg Kastning

- Verdienne mein Geld seit 2003 mit EDV/IT
- Seit März 2023 als Mitglied der Red Hat TAM-Community
- Ein TAM ist ein Technical Account Manager
- Benutze Vim; habe Emacs nie verstanden
- Bin ein 1x Engineer, Blogger, TAM-Ambassador, ...



Christian Patchowie Stankowic

- IT-Berater und -Trainer bei SVA GmbH
- Linux, Infrastructure as Code, Python
- Patch-Management seit 2014 (Spacewalk)
- sammelt ~~Elektroschrott~~ Retro-Hardware
- Bloggt (cstan.io) und podcastet, u.a.
- Urlaub im Userspace, ThinkPad-Museum
- schreibt fürs Linux-Magazin



Abschnitt

Schwachstellen-Management

Entwicklung der Schwachstellenanzahl

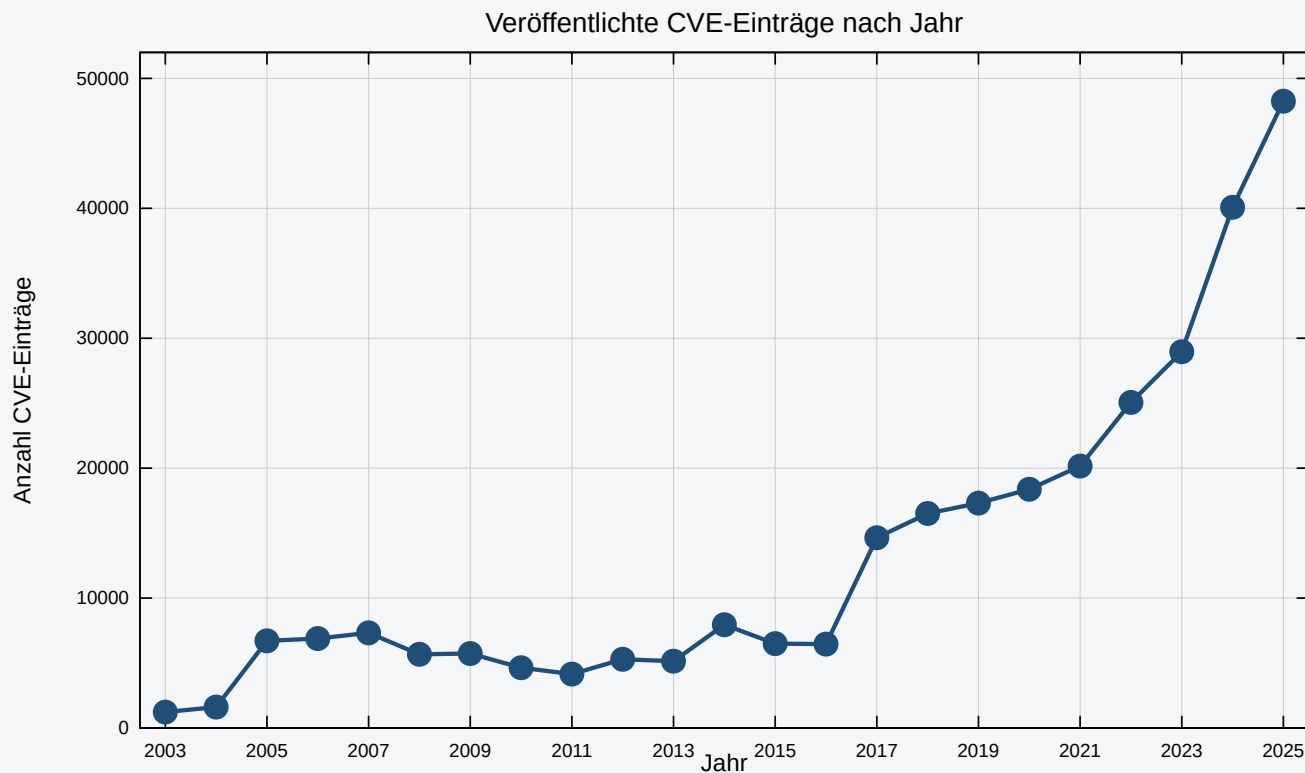


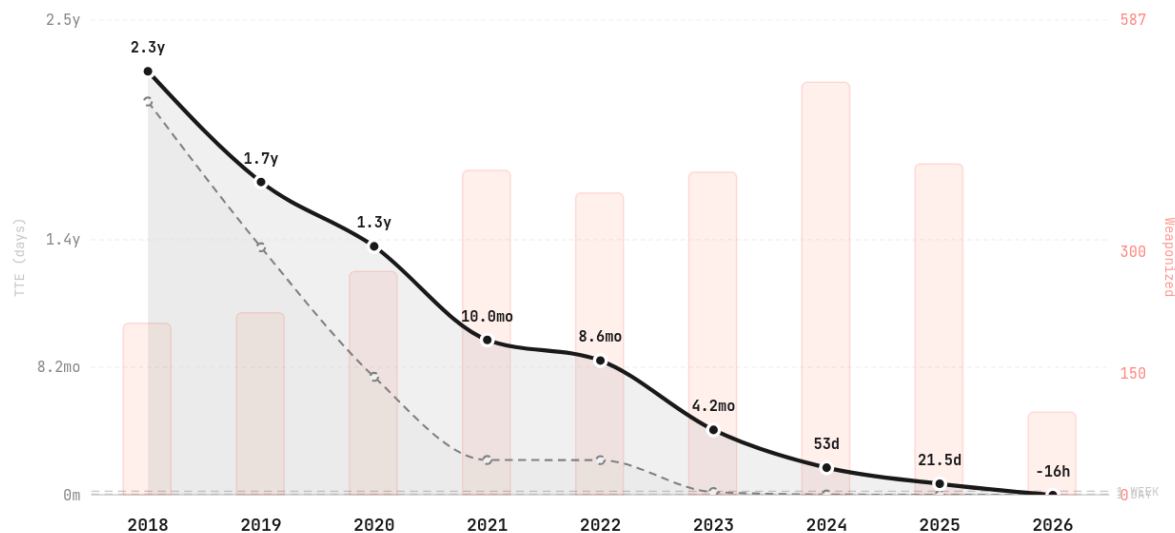
Abb. 1: Entwicklung der Schwachstellenanzahl [1]

Die Uhr tickt

From Vulnerability to Exploitation

TTE measures the gap between CVE public disclosure and first confirmed in-the-wild exploitation. Zero = same-day.

— Mean TTE (10% trimmed, days) - - - Median TTE (days) ■ Weaponized Exploits (count)



Based on 3,500+ confirmed-exploited CVEs (CISA KEV + VulnCheck KEV, with VulnCheck XDB timestamps for early-year CVEs)

● zerodayclock.com

Die Uhr tickt

Time-to-Exploit Milestones

Projected year when median TTE crosses each threshold — extrapolated from observed 2018–2024 trend

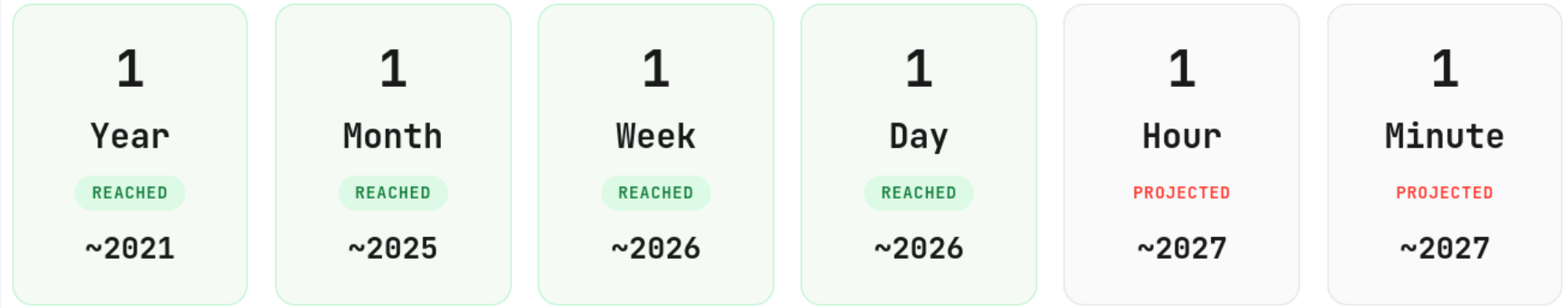


Abb. 2: Diagramme von Zerodayclock [2]

Common Vulnerability Scoring System (CVSS)

Definition und Verweise:

- Der CVSS ist ein allgemeines Bewertungssystem für Schwachstellen [3].
- CVSS gibt es in den Versionen 2, 3 und 4 [4], wobei Version 3 aktuell die gebräuchlichste ist.
- Spezifikation und Verwaltung finden bei der CVSS SIG [5] statt.
- Risiko: Wie wahrscheinlich ist es, dass ein Schaden eintritt?
- Schweregrad: Wie schlimm ist es, wenn ein Schaden eintritt?

Common Vulnerability Scoring System (CVSS)

Qualitative Schweregrade nach CVSS v3:

Severity	CVSSv3 Range
None	0,0
Low	0,1-3,9
Medium	4,0-6,9
High	7,0-8,9
Critical	9,0-10,0

Tabelle 1: Abstufungen der CVSSv3-Schweregrade [4]

Common Vulnerability Scoring System (CVSS)

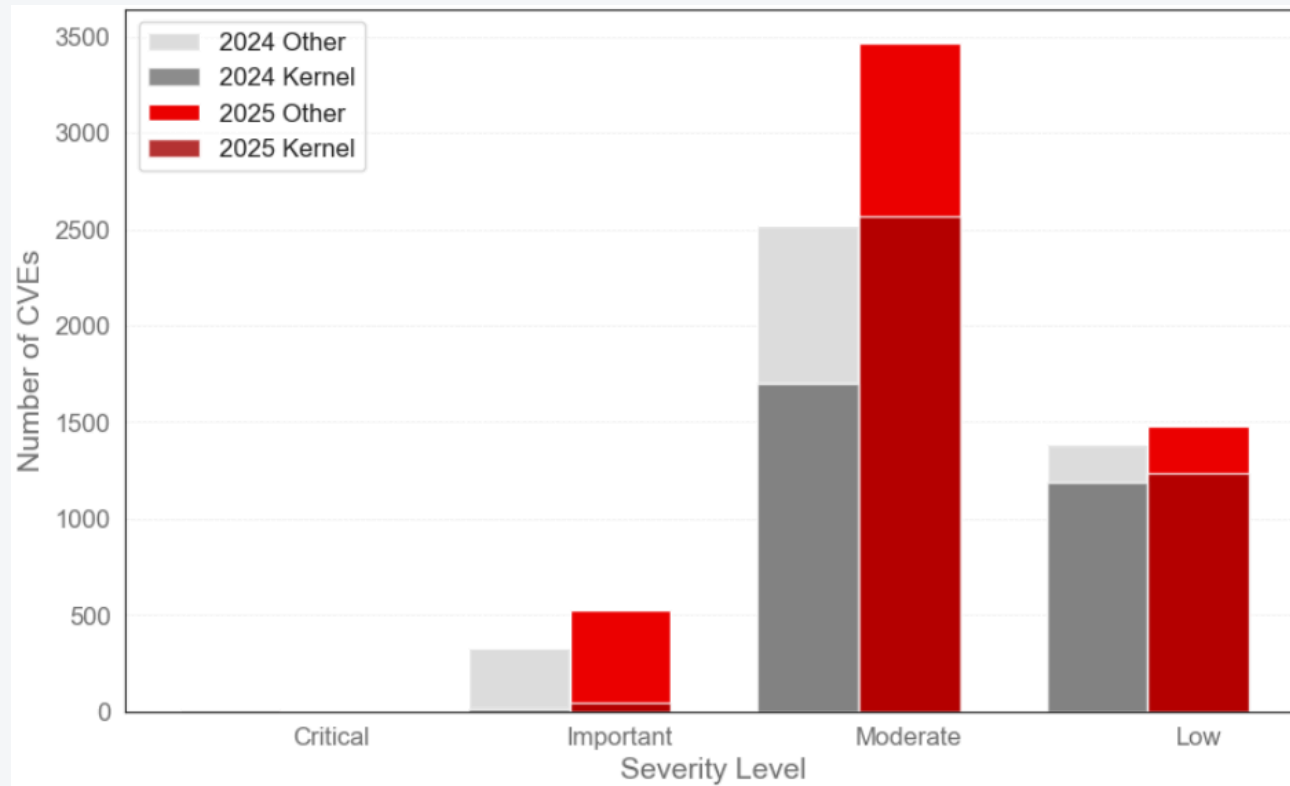


Abb. 3: Entwicklung und Verteilung in den Jahren 2024 und 2025 [6].

Abschnitt

Patch-Management-Konzepte

Herausforderungen und Spannungsfelder

- **Verantwortung:** Wer patcht das Betriebssystem und wer die Anwendung?
- **Erfolgskontrolle:** Funktioniert es hinterher noch wie es soll?
- **Rahmenbedingungen:** SLA, Wartungsfenster, Abhängigkeiten, etc.

Beispiel 1

Phase A

Warungsfenster planen

1 pro Quartal; 1 Jahr Vorlauf, meist am Wochenende

Phase B

Update in DEV/TEST

Installation aller Updates; 2 Wochen Beobachtung, ob es knallt

Phase C

Update in PROD

Installation der gleichen Updates wie in DEV/TEST

Beispiel 1

Anmerkungen

- Kein Ablaufplan für Notfälle
-
-
-
-
-

Beispiel 1

Anmerkungen

- Kein Ablaufplan für Notfälle
- Kein standardisiertes Verfahren für die DMZ
-
-
-
-

Beispiel 1

Anmerkungen

- Kein Ablaufplan für Notfälle
- Kein standardisiertes Verfahren für die DMZ
- Abhängigkeiten nicht sauber dokumentiert
-
-
-

Beispiel 1

Anmerkungen

- Kein Ablaufplan für Notfälle
- Kein standardisiertes Verfahren für die DMZ
- Abhängigkeiten nicht sauber dokumentiert
- Viele manuelle Schritte
-
-

Beispiel 1

Anmerkungen

- Kein Ablaufplan für Notfälle
- Kein standardisiertes Verfahren für die DMZ
- Abhängigkeiten nicht sauber dokumentiert
- Viele manuelle Schritte
- Hoher Kommunikationsaufwand
-

Beispiel 1

Anmerkungen

- Kein Ablaufplan für Notfälle
- Kein standardisiertes Verfahren für die DMZ
- Abhängigkeiten nicht sauber dokumentiert
- Viele manuelle Schritte
- Hoher Kommunikationsaufwand
- **Ziel:** Automatisierung des Verfahrens; es sollen jeden Tag Updates ausgerollt werden können

Beispiel 1

Erwartungen

Severity	Zbl ¹
None	–
Low	3 Monate
Medium	4 Wochen
High	5 Tage
Critical	48 Std. ²

Tabelle 2: Vorgabe der IT-Sicherheits-Abteilung zur Installation von Sicherheitsupdates.

¹Zeit bis zur Installation

²Soll auf 3 Std. sinken

Beispiel 2

Phase A

Warungsfenster planen

1 Patchzyklus alle 2 Wochen; alle Nächte und Wochenenden sind genehmigte Wartungsfenster; nur wenige Ausnahmen

Phase B

Installation in TEST

Installation aller Updates, 4 Tage automatisierte Tests, Prometheus-Monitoring

Phase C

Installation in PROD

Installation aller Updates; Monitoring dient zur Prüfung, ob alle Dienste OK sind.

Beispiel 2

Anmerkungen

- Automatisierungsgrad liegt bei ca. 80%, mit Berücksichtigung von Abhängigkeiten, Cluster-Schwenks, Monitoring
- Die 20% Sonderfälle werden manuell oder semi-automatisch (Ansible) aktualisiert
- Beschleunigtes Notfall-Verfahren; Zeit zwischen TEST und PROD auf 1 Tag reduziert
- IT-Sicherheitsabteilung entscheidet, wann ein Notfall vorliegt
- Ist kein Neustart erforderlich, können Updates jederzeit/sofort verteilt werden

Beispiel 2

Erwartungen

- Mehr Test; verbesserte Tests
- Verbesserung Monitoring
- Steigerung des Automatisierungsgrades

Abschnitt

Patch-Management-Werkzeuge

Patch-Management-Werkzeuge

- es gibt eine **Vielzahl** an Open-Source Tools und Suites, die hier helfen
 - von kleinen bis hin zu sehr großen Umgebungen
 - Features variieren, für jede:n etwas dabei 😊

Patch-Management-Werkzeuge

- es gibt eine **Vielzahl** an Open-Source Tools und Suites, die hier helfen
 - von kleinen bis hin zu sehr großen Umgebungen
 - Features variieren, für jede:n etwas dabei 😊
- häufig existieren bereits **proprietäre** Patch-Management-Werkzeuge
 - z.B. für Microsoft Windows-Systeme
 - manche davon haben Linux-Support, i.d.R. ist dieser nicht gut

Patch-Management-Werkzeuge

- es gibt eine **Vielzahl** an Open-Source Tools und Suites, die hier helfen
 - von kleinen bis hin zu sehr großen Umgebungen
 - Features variieren, für jede:n etwas dabei 😊
- häufig existieren bereits **proprietäre** Patch-Management-Werkzeuge
 - z.B. für Microsoft Windows-Systeme
 - manche davon haben Linux-Support, i.d.R. ist dieser nicht gut
- es existieren auch Enterprise-Werkzeuge mit **Support**
 - Red Hat Satellite, SUSE Multi-Linux Manager, ATIX orcharhino
 - zahlreiche zusätzliche Features und wertvolle Integrationen

Patch-Management-Werkzeuge: kleine Umgebungen

	SUSE RMT [7]	Aptly [8]	Repomanager [9]
Erstes Release	2018	2013	2021
Tech-Stack	Ruby, MariaDB, NGINX	Golang	PHP, NGINX, SQLite
Distributionen	SLES, openSUSE Leap	Debian-like	Debian, Ubuntu, RHEL-like
Client benötigt	ja	nein	ja (linupdate)
Web-Oberfläche	nein	nein	ja
Staging	nein	ja	ja

SNAPSHOT

REPOSITORY

debian-security > bookworm-security > main new

SNAPSHOT

02-03-2026

SIZE

19G

PACKAGES

2333

+ cache

+ dists

- pool

- main

activemq_5.17.2+dfsg-2+deb12u1_all.deb

50K

aide-common_0.18.3-1+deb12u4_all.deb

106K

aide-dynamic_0.18.3-1+deb12u4_all.deb

33K

aide_0.18.3-1+deb12u4_amd64.deb

132K

aom-tools_3.6.0-1+deb12u1_amd64.deb

156K

apache2-bin_2.4.62-1~deb12u2_amd64.deb

2M

apache2-data_2.4.62-1~deb12u2_all.deb

157K

UPLOAD PACKAGES

SELECT PACKAGES TO UPLOAD

Max upload size: 64M

Valid MIME types: application/x-rpm and application/vnd.debian.binary-package

Sélect. fichiers

Aucun fichier choisi

Upload package

REBUILD REPOSITORY

SIGN WITH GPG

Signature can extend the task duration.

☒

Execute

Abb. 4: Über Repomanagers UI lassen sich u.a. Repositories stagen

24 / 37

Patch-Management-Werkzeuge: Suiten

	Foreman [10]/Katello [11]	Uyuni [12]
Erstes Release	2009/2014	2018
Tech-Stack	Tomcat, PostgreSQL, Redis	Tomcat, PostgreSQL, Salt, Podman
Distributionen	RHEL-/Debian-like, Fedora	SUSE, RHEL-like, Debian, Ubuntu
Client benötigt	nein (SSH)	ja (Salt)
Web-Oberfläche	ja	ja
Staging	ja	ja
Configuration Management	Ansible, Salt, OpenVox	Salt, Ansible

Patch-Management-Werkzeuge: Suiten

	Foreman [10]/Katello [11]	Uyuni [12]
Bereitstellung neuer Systeme	PXE, Hypervisor, Cloud	PXE
RBAC	ja	ja
REST API	ja	ja (XMLRPC, JSON)
Automatisierung	CLI (hammer), Ansible, Terraform (inoffiziell)	CLI (spacecmd), Ansible und Terraform (inoffiziell)
Authentifizierung	Lokale User, LDAP/Microsoft AD-DS	
Security	OpenSCAP-Audits, Mandantenfähig	

FOREMAN Weyland Kalifornien Admin User

Search and go

- Monitor
- Content
- Hosts
- Configure
- Infrastructure
- Administer

Hosts > katello-client.homelab.loc

katello-client.homelab.loc AlmaLinux 9.6 x86_64

Schedule a job Edit

Created 5 months ago by Anonymous Admin (updated 8 hours ago)

Overview Details Content Parameters Traces Ansible Reports

Host status

1 0 1 4

Manage all statuses

Content view environment

Library rcv-almalinux9

Errata Applicable Installable

21 errata

20 security advisories
1 bug fix
0 enhancements

Details

IPv6 address
Not available

IPv4 address
192.168.13.37

MAC address
00:50:56:bb:4b:72

Host group

Recent jobs

Finished	Running	Scheduled
Run uptime	14 days ago	succeeded
Install errata errata_id ^ (AL...	14 days ago	succeeded
Install errata ALSA-2025:18...	1 month ago	succeeded

Recent communication

Last configuration Never

Host collections

Abb. 5: Ein über Foreman/Katello verwaltetes System

Uyuni > Systems > System List > All

Search page

Home

Systems

System List

All

Physical Systems

Virtual Systems

Unprovisioned Systems

Out of Date

Requiring Reboot

Non Compliant

Ungrouped

Inactive

Recently Registered

Proxy

Duplicate Systems

System Currency

System Types

System Groups

System Set Manager

Bootstrapping

Proxy Configuration

Advanced Search

Activation Keys

Stored Profiles

Uyuni release 2025.10

SUSE

Systems

+ Add system

System

Download CSV

	System	Updates	Patches	Packages	Extra Packages	Config Diffs	Last Checked In	Base Channel	System Type
☐	 almalinux-client.homelab.loc 	41	471	471	0		Nov 26, 2025, 4:00:01 AM	AlmaLinux 9 (x86_64)	Salt, Monitor this Host
☐	 uyuni-client.homelab.loc 	325	375	2	0		Nov 26, 2025, 11:00:01 AM	os-clients-dev-openSUSE Leap 15.6 (x86_64)	Salt, Monitor this Host
☐	 uyuni-proxy.homelab.loc 	13	36	126	0		Nov 26, 2025, 12:00:01 AM	openSUSE Leap Micro 6.2 (x86_64)	Salt, Proxy

Items 1 - 3 of 3

Abb. 6: Über Uyuni inventarisierte Systeme

Patch-Management-Werkzeuge: Enterprise

	Red Hat Satellite [13]	ATIX orcharhino [14]	SUSE Multi-Linux Manager [15]
Basis	früher Spacewalk, Foreman/Katello	Foreman/Katello	Uyuni
Erstes Release	2002	2016	2012
Zyklus	6 Monate	~2 Monate	12 Monate
Wartung	1,5 Jahre	n - 2	3 Jahre
Subskribierung	Managed Systems (RHEL with Smart Management)	Server + Managed Systems (50/1000)	Managed Systems (Lifecycle Management+)
Support-Level	9x5, 24x7		

Red Hat Satellite

Reynholm Industries

London

Admin User

Search and go

Monitor

Content

Hosts

Red Hat Lightspeed

Configure

Infrastructure

Administer

Hosts

satellite-client.homelab.loc

satellite-client.homelab.loc

RedHat 9.5

x86_64

Schedule a job

Edit

Created 3 minutes ago by Anonymous Admin (updated 1 minute ago)

OverviewDetailsContentParametersTracesAnsibleReports

PackagesErrataModule streamsRepository sets

Search

→

Security

Severity

Apply

1 - 20 of 180

Errata	Type	Severity	Installable	Synopsis	Published date
▶ ☐ RHSA-2025:22175	🛡️ Security	🔴 Important	✓ Yes	Important: exp...	11/26/2025
▼ ☐ RHSA-2025:22011	🛡️ Security	🔴 Important	✓ Yes	Important: buil...	11/25/2025
▶ Bugs2 ▶ CVEs2 ▶ Packages2 ▶ Module streams0 Synopsis Important: buildah security update Summary An update for buildah is now available for Red Hat Enterprise Linux 9. Red Hat Product Security has rated this update as having a security impact of Important. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) in the References section. Solution For details on how to apply this update, which includes the changes described in this advisory, refer to: https://access.redhat.com/articles/11258					

Abb. 7: Red Hat Satellite ähnelt Foreman nicht nur optisch

SUSE® Multi-Linux Manager > Home > Overview

🔔 🔍 1 system selected ✍️ 👤 admin 👥 Homelab ⚙️ ➡️

Search page 🔍

🏠 Home ^

Overview

Notification Messages

User Account v

My Preferences

My Organization v

🖥️ Systems v

📦 Salt v

📄 Images v

🔧 Patches v

👥 Software v

📅 Content Lifecycle v

🔍 Audit v

⚙️ Configuration v

🕒 Schedule v

👥 Users v

👤 Admin v

SUSE Multi-Linux Manager release 5.1.0 🐉

👥 Overview ⓘ

⚠️ You have subscriptions that are expiring soon or already expired. Please check the [Subscription Matching](#) page.

Tasks

▸ Manage System Types:
[My Organization](#)

▸ [Register Systems](#)

▸ [Manage Activation Keys](#)

▸ [Manage Autoinstallations](#)

▸ [Manage Configuration Files](#)

▸ [Manage Organizations](#)

▸ [Configure SUSE Multi-Linux Manager](#)

Inactive Systems

No inactive systems.

All of your systems are actively checking into SUSE Multi-Linux Manager at this time. You can view a list of all of your systems at [Systems > All](#).

Most Critical Systems

System	All Updates	Security Patches	Bugfix Patches	Enhancement Patches
suma-client.homelab.loc	137	🛡️ 73	🐛 60	📦 4

1 - 1 of 1 most critical systems displayed [View All Critical Systems](#)

Recently Scheduled Actions

Action	User	Age
✅ Hardware List Refresh	(none)	17 Day(s)

Abb. 9: SUSE Multi-Linux Manager ähnelt Uyuni technisch und optisch

33 / 37

Wann welches Patch-Management-Werkzeug nutzen?

- Homogene SUSE- oder Red Hat-Landschaft
 - SUSE Multi-Linux Manager oder Red Hat Satellite

Wann welches Patch-Management-Werkzeug nutzen?

- Homogene SUSE- oder Red Hat-Landschaft
 - SUSE Multi-Linux Manager oder Red Hat Satellite
- Heterogene Landschaft, viele Distributionen (SLES, RHEL, Ubuntu,...)
 - SUSE Multi-Linux Manager oder ATIX orcharhino

Wann welches Patch-Management-Werkzeug nutzen?

- Homogene SUSE- oder Red Hat-Landschaft
 - SUSE Multi-Linux Manager oder Red Hat Satellite
- Heterogene Landschaft, viele Distributionen (SLES, RHEL, Ubuntu,...)
 - SUSE Multi-Linux Manager oder ATIX orcharhino
- ...wird zusätzlich ein hohes Maß an Automatisierung benötigt?
 - ATIX orcharhino

Wann welches Patch-Management-Werkzeug nutzen?

- Homogene SUSE- oder Red Hat-Landschaft
 - SUSE Multi-Linux Manager oder Red Hat Satellite
- Heterogene Landschaft, viele Distributionen (SLES, RHEL, Ubuntu,...)
 - SUSE Multi-Linux Manager oder ATIX orcharhino
- ...wird zusätzlich ein hohes Maß an Automatisierung benötigt?
 - ATIX orcharhino
- wenn kein Support gewünscht ist, können auch die Upstream-Projekte verwendet werden
- späterer Wechsel auf Enterprise-Version kann automatisiert werden

Abschnitt

Fazit und Q&A

Fazit und Q&A

- Patch-Management ist **unabdingbar**, insbesondere in Zeiten von LLM-beschleunigten CVEs und Exploits
- Lückenlose **Dokumentation** von Verantwortlichkeiten und Rahmenbedingungen notwendig
- Verlässliches **Monitoring** entscheidend für eine schnelle Prüfung auf Erfolg
- Manuelle Arbeiten (Vorbereitung, Durchführung und Kontrolle) **automatisieren**
- Einsatz eines Patch-Management-Werkzeugs, welches die eigenen **Anforderungen abdeckt**
- Regelmäßige erneute Evaluation des Vorgehens (KISS-Prinzip?)

Vielen Dank.

Fragen?

Quellen und Verweise

- [1] “Published CVE Records.” [Online]. Available: <https://www.cve.org/About/Metrics>
- [2] “Zero Day Clock.” [Online]. Available: <https://zerodayclock.com/>
- [3] “CVSS - Wikipedia.” [Online]. Available: <https://de.wikipedia.org/wiki/CVSS>
- [4] “Vulnerability Metrics - National Vulnerability Database.” [Online]. Available: <https://nvd.nist.gov/vuln-metrics/cvss>
- [5] “Common Vulnerability Scoring System SIG.” [Online]. Available: <https://www.first.org/cvss/>

- [6] “Red Hat Product Security Risk Report 2025.” [Online]. Available: <https://www.redhat.com/en/resources/product-security-risk-report-2025>
- [7] “SUSE Repository Mirroring Tool.” [Online]. Available: <https://documentation.suse.com/sles/15-SP7/html/SLES-all/rmt-overview.html>
- [8] “Aptly.” [Online]. Available: <https://www.aptly.info/>
- [9] “Repomanager.” [Online]. Available: <https://github.com/lbr38/repomanager>
- [10] “Foreman.” [Online]. Available: <https://theforeman.org/>

- [11] “Katello-Plugin.” [Online]. Available: <https://theforeman.org/plugins/katello/>
- [12] “Uyuni.” [Online]. Available: <https://uyuni-project.org/>
- [13] “Red Hat Satellite.” [Online]. Available: <https://www.redhat.com/en/technologies/management/satellite>
- [14] “ATIX orcharhino.” [Online]. Available: <https://orcharhino.com/>
- [15] “SUSE Multi-Linux Manager.” [Online]. Available: <https://www.suse.com/products/multi-linux-manager/>