

Schwachstellenmanagement 2026

Wer sagt uns eigentlich, was kaputt ist?

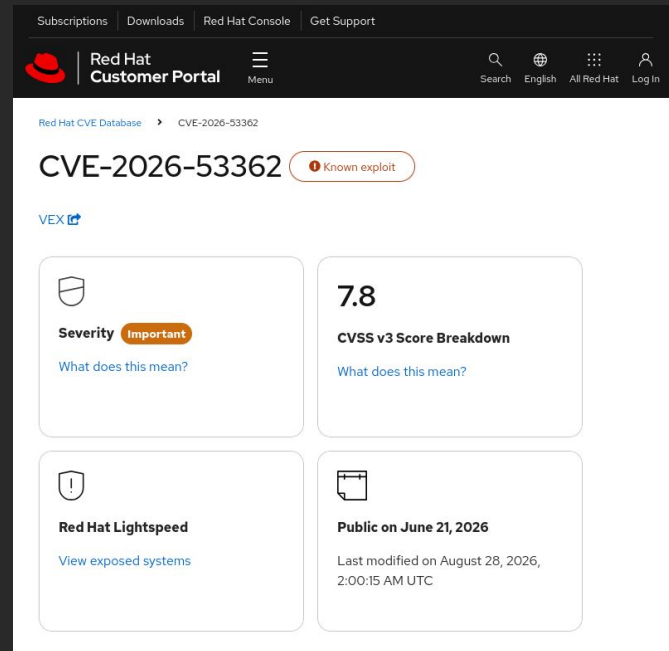
Julian Jakobs
Technical Account Manager

Enterprise Linux Anwendertreffen
29.09.2026



Was machen wir damit?

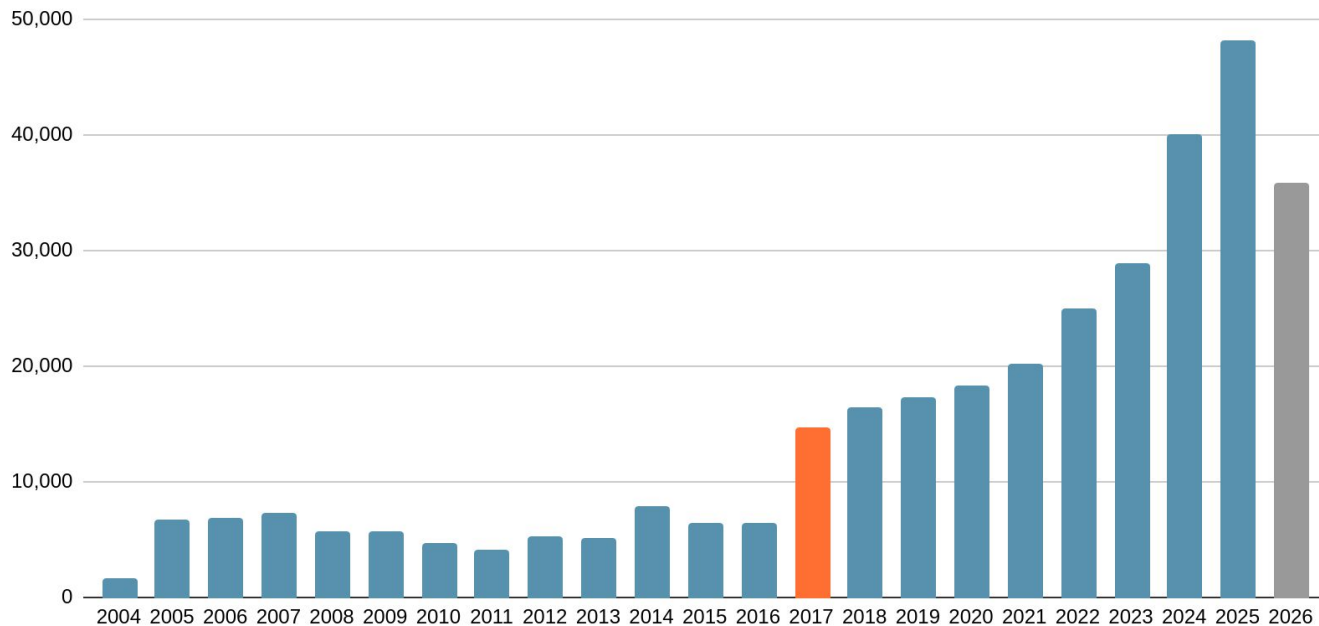
- ▶ CVE-2026-53362 „IPV6_FRAG_ESCAPE“ im Linux-Kernel
- ▶ Lokale Rechteausweitung
- ▶ Container Escape
- ▶ Severity: Important



The screenshot shows the Red Hat Customer Portal interface for CVE-2026-53362. The page header includes navigation links for Subscriptions, Downloads, Red Hat Console, and Get Support. The main header features the Red Hat logo, the text 'Red Hat Customer Portal', a menu icon, and search, language, and login options. The breadcrumb trail indicates the path: Red Hat CVE Database > CVE-2026-53362. The title 'CVE-2026-53362' is prominently displayed with a 'Known exploit' badge. Below the title, a 'VEX' link is visible. The page is divided into four informational cards: 1. Severity: Important (with a shield icon and a link to 'What does this mean?'). 2. CVSS v3 Score Breakdown: 7.8 (with a link to 'What does this mean?'). 3. Red Hat Lightspeed (with a shield icon and a link to 'View exposed systems'). 4. Public on June 21, 2026 (with a document icon and the text 'Last modified on August 28, 2026, 2:00:15 AM UTC').



Zwanzig Jahre CVE-Veröffentlichungen



Was die Zahlen tatsächlich sagen

H1 2026 verglichen mit H2 2025

Veröffentlichte CVEs:

+45 %

Neue VulnCheck-KEV-Einträge:

+10 %



Der Plan:

lesen, entscheiden, automatisieren

- ▶ Akt 1. Wer sagt uns was?

Sieben Quellen und was jede davon gerade nicht aussagt.

- ▶ Akt 2. Was könnt ihr damit machen?

Vom Inventar über den Abgleich bis zum Nachweis, dass der Fix wirkt.

- ▶ Akt 3. Pflicht und Anschluss

NIS2 und CRA, Meldefristen und was ihr von Lieferanten braucht.



Sieben Aussagen über dieselbe Schwachstelle

Wer sagt es	Was sagt es	Was es nicht sagt
CVE-ID CNA	es gibt einen Fehler und er hat einen Namen	keine Bewertung
CVSS CNA / NVD / Scanner	technische Eigenschaft im ungünstigsten Fall	nicht euer Risiko
Hersteller-Rating Hersteller	der Hersteller bewertet sein Produkt wie ausgeliefert	nicht euren Eigenbau
Paketstand Hersteller + euer System	dieser Fix ist in diesem Release enthalten	nicht die Upstream-Versionsnummer
VEX Hersteller	Status für ein Produkt, mit Begründung und Stand	kein Inventarabgleich
KEV CISA / VulnCheck	es gibt einen Ausnutzungsnachweis	kein Ausschluss bei fehlendem Eintrag
EPSS FIRST	Wahrscheinlichkeit über die Grundgesamtheit	keine Aussage über euch



CVE-ID und CVSS

Ein Name und eine Eigenschaft



CVE-ID · das Namensschild

Vergeben von einer CNA (CVE Numbering Authority),
inzwischen über 450 Organisationen, darunter Red Hat.

Sagt: es gibt einen Fehler, und wir meinen alle denselben.



CVSS · die Eigenschaft, kein Risiko

Base Score: Annahmen über Angreifer und
Umgebung, nicht über eure.

Seit April 2026 ergänzt die NVD keinen eigenen zweiten Score
mehr, wenn die CNA schon einen geliefert hat.

Wer einen Score übernimmt, sollte dessen Herkunft und Stand kennen.



Herstellerrating

9.8 und Moderate zugleich

- ▶ CVE-2023-3128: Grafana
- ▶ Red Hat: CVSS 3.1 = 9.8
- ▶ Severity = Moderate
- ▶ Begründung: Azure-AD-Zugang standardmäßig deaktiviert
- ▶ Die Konfiguration entscheidet mit

Das ist kein Streit zwischen zwei Datenbanken.
Das sind zwei verschiedene Fragen.

Red Hat CVE Database > CVE-2023-3128

CVE-2023-3128

VEX 



Severity **Moderate**

[What does this mean?](#)

9.8

CVSS v3 Score Breakdown

[What does this mean?](#)

Jump

Description Statement Mitigation Affected Pa

Description

A flaw was found in Grafana, which validates Azure AD accounts based on the email claim. On Azure AD, the profile email field is not unique across Azure AD tenants, which enables Grafana account takeover and authentication bypass when Azure AD OAuth is configured with a multi-tenant AzureAD OAuth application. This may allow an attacker to gain complete control of the user's account, including access to private customer data and sensitive information.

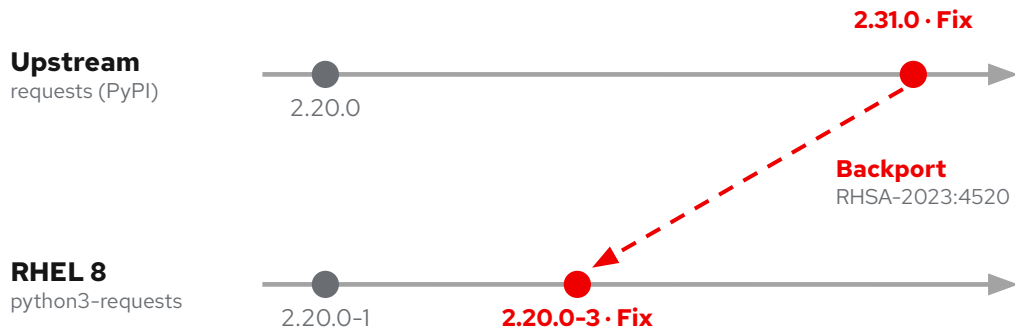
Statement

The vulnerability affecting Red Hat Enterprise Linux 8 and 9 has been categorized as moderate primarily because Azure Active Directory access is not supported by default in Grafana configurations. Specifically, it remains disabled in the Grafana configuration file located at `/etc/grafana/grafana.ini` within the Azure AD section. Even if someone were to enable Azure Active Directory access, they retain the option to easily revert it back to the default state, ensuring it remains disabled.



Backporting: CVE-2023-32681 in python-requests

Die Versionsnummer allein lügt



Scanner, der nur Versionen vergleicht:

2.20.0 < 2.31.0 → verwundbar ✗ falsch

```
$ rpm -q python3-requests
python3-requests-2.20.0-3.el8_8.noarch

$ rpm -q --changelog python3-requests \
  | grep CVE-2023-32681
- Security fix for CVE-2023-32681
```

Der Paketstand verrät den Fix, die Versionsnummer nicht.

Die Lücke: requests reicht bei Redirects den Proxy-Authorization-Header an das Ziel weiter.



VEX

Status, Geltungsbereich, Stand

VEX beantwortet: Betrifft diese CVE dieses Produkt?

- ▶ Produkt + Version + CVE + Status + Begründung + Stand

betroffen

nicht betroffen

beheben

in Untersuchung

- ▶ Kein Eintrag ≠ nicht betroffen
- ▶ Produktstatus mit dem eigenen Inventar verbinden
- ▶ Red Hat liefert VEX als CSAF, dazu OVAL und eine Security-Data-API
- ▶ öffentlich, ohne Subskription



EPSS und KEV: Prognose und Beleg

EPSS: wird wohl ausgenutzt

Eine Prognose über die
Grundgesamtheit.
Nicht über euch.

KEV: Ausnutzung ist dokumentiert

Ein Nachweis.
Kein Eintrag ist kein Ausschluss.

Eigene Angriffsspuren

Dann ist es zu spät fürs Patchen.
→ Incident Response!

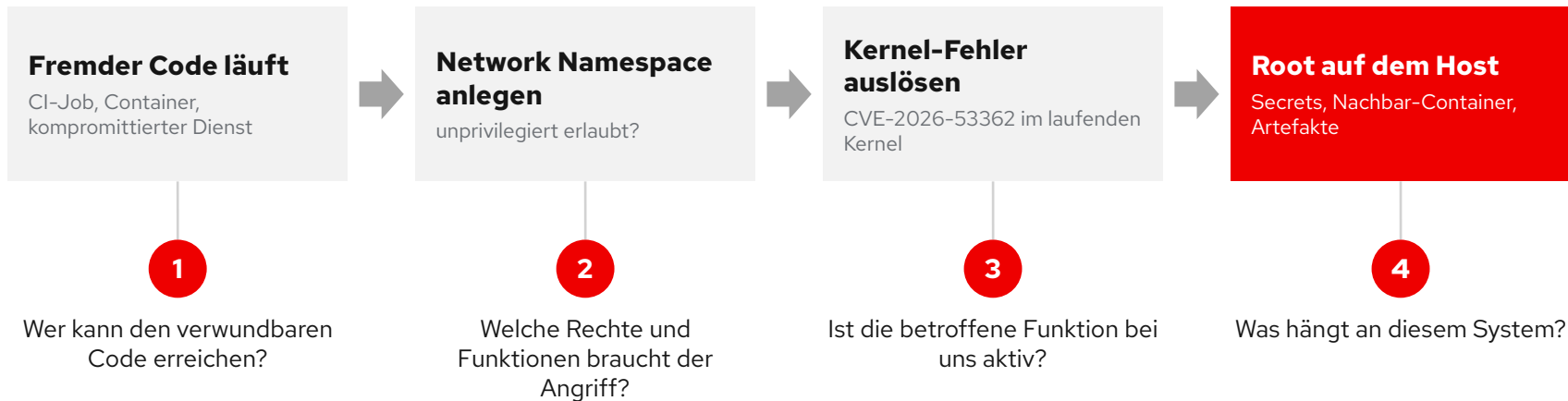
Prognose · irgendwo

Beleg · irgendwo

Beleg · bei euch



Eure Priorität ist die einzige Zahl im Ticket



Kein Schritt in diesem Pfad braucht das Internet.
„Nicht aus dem Internet erreichbar“ ist keine Entwarnung.



Sieben Aussagen über dieselbe Schwachstelle

Wer sagt es	Für CVE-2026-53362
CVE-ID	es gibt den Fehler, wir meinen alle denselben
CVSS	7.8: hohe technische Schwere, ohne unseren Kontext
Hersteller-Rating	Important, für RHEL wie ausgeliefert
Paketstand	betrifft den laufenden Kernel, nicht den installierten
VEX	RHEL 10 betroffen, RHEL 9 nicht betroffen, Fixes veröffentlicht
KEV	kein Eintrag, also keine Aussage
EPSS	Prognose, kein Urteil über uns

```
$ rpm -q kernel
kernel-6.12.0-55.9.1.el10_0.x86_64
kernel-6.12.0-55.20.1.el10_0.x86_64
$ uname -r
6.12.0-55.9.1.el10_0.x86_64
$ dnf needs-restarting -r
Updating Subscription Management repositories.
Core libraries or services have been
updated since boot-up:
* kernel
Reboot is required to fully utilize these updates.
More information:
https://access.redhat.com/solutions/27943
```

Installiert ≠ läuft.

Bei einem Kernel zählt nur der laufende.

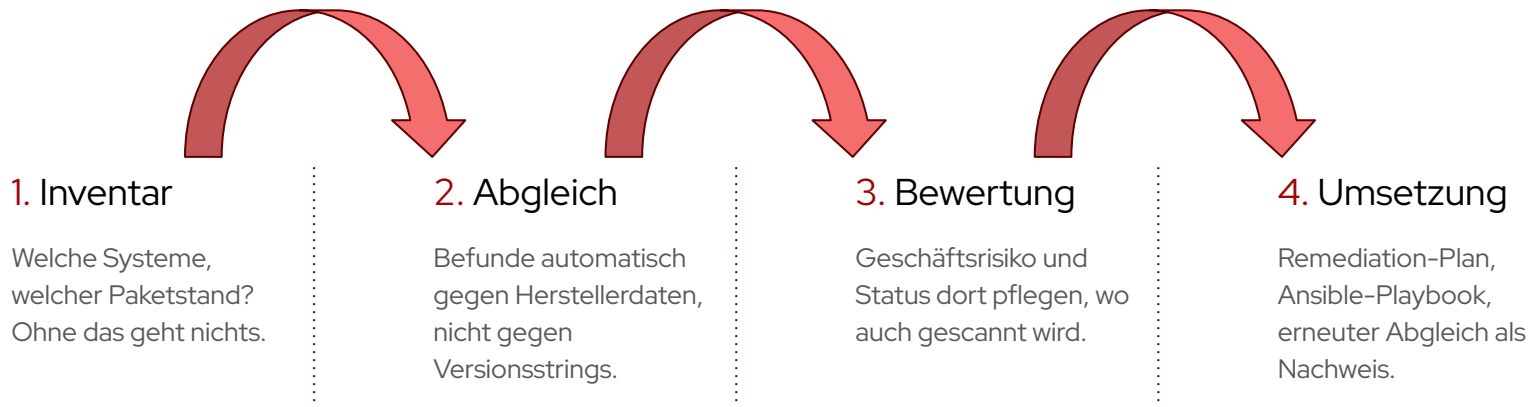


Und wer macht das jetzt
für zweitausend Hosts?

Und für die nächsten 48.000 CVEs?



Vier Stufen, die aufeinander aufbauen



Jede Stufe ist ohne die vorherige wertlos. Stufe 4 ohne Stufe 1 ist Patchen im Blindflug.



Stufe 1

Ein Inventar, dem ihr glaubt

- Welche Hosts, welche RHEL-Version, welcher Paketstand, welcher laufende Kernel?
- Welche Container-Images, mit welchem Digest, aus welchem Build?
- Welche Software kam **nicht** aus den Repositories?

Der Tag „:latest“ ist keine Inventarangabe.



Stufe 2

Den Abgleich die Maschine machen lassen

Der Vulnerability-Service von Red Hat Lightspeed – Abgleich gegen Red-Hat-CVE-Daten und Security Bulletins.

Host

insights-client

Abgleich gegen
Red Hat Daten

Befund + Status

vulnerable

betroffen und angreifbar

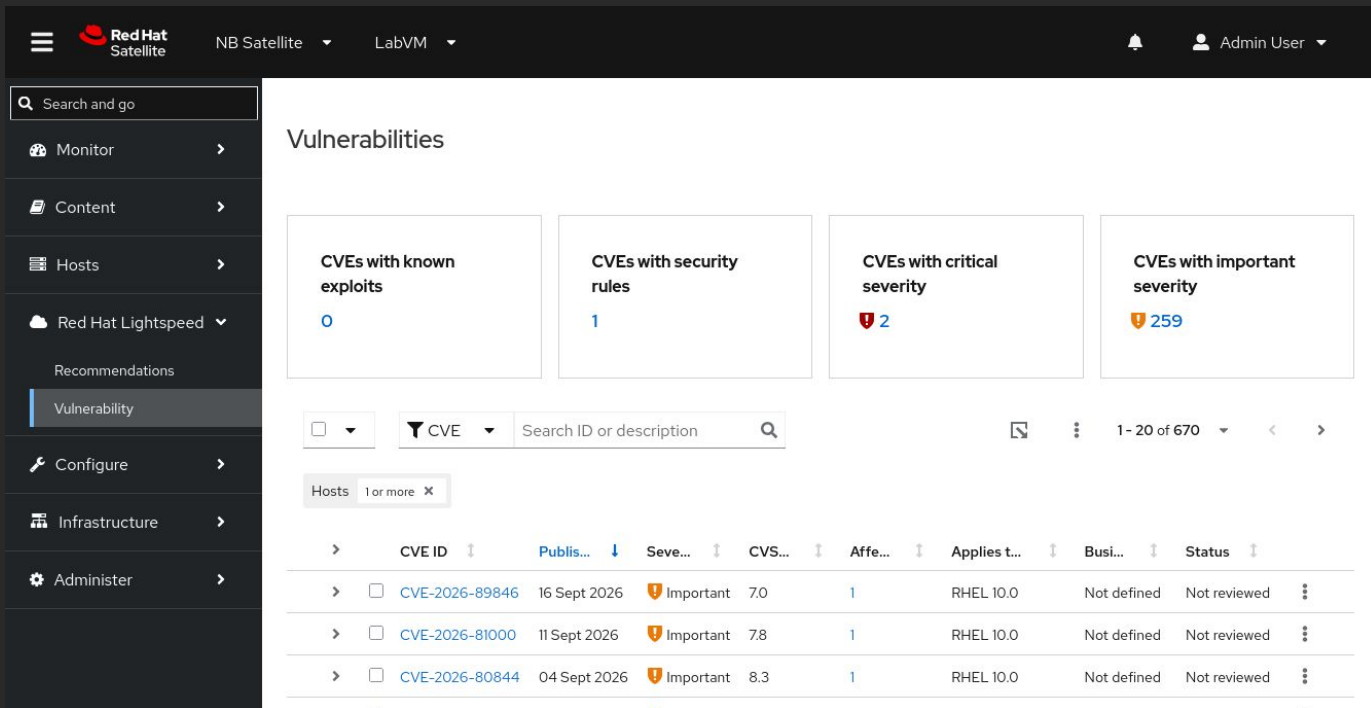
Affected but not vulnerable

Betroffen, aber hier nicht ausnutzbar



Lightspeed on premise

der Abgleich bleibt im Haus



Red Hat Satellite NB Satellite LabVM Admin User

Search and go

Monitor >

Content >

Hosts >

Red Hat Lightspeed >

Recommendations

Vulnerability

Configure >

Infrastructure >

Administer >

Vulnerabilities

CVEs with known exploits
0

CVEs with security rules
1

CVEs with critical severity
2

CVEs with important severity
259

☐ CVE Search ID or description

Hosts 1 or more x

>	CVE ID	Publis...	Seve...	CVS...	Affe...	Applies t...	Busi...	Status
>	☐ CVE-2026-89846	16 Sept 2026	Important	7.0	1	RHEL 10.0	Not defined	Not reviewed
>	☐ CVE-2026-81000	11 Sept 2026	Important	7.8	1	RHEL 10.0	Not defined	Not reviewed
>	☐ CVE-2026-80844	04 Sept 2026	Important	8.3	1	RHEL 10.0	Not defined	Not reviewed



Lightspeed on premise

der Abgleich bleibt im Haus

The screenshot displays the Red Hat Satellite Lightspeed interface. The top navigation bar includes the Red Hat Satellite logo, environment selectors for 'NB Satellite' and 'LabVM', and a user profile for 'Admin User'. A left-hand sidebar contains navigation links: Monitor, Content, Hosts, Red Hat Lightspeed (expanded to show Recommendations and Vulnerability), Configure, Infrastructure, and Administer. The main content area features a search bar and an 'Actions' dropdown. The primary focus is on the CVE-2026-53362 entry, which includes its publish date (21 June 2026), a detailed description of a flaw in the Linux kernel's ipv6 networking subsystem, and a severity rating of 'Important' with a CVSS 3.0 base score of 7.8. Below this, a table lists affected systems, with one entry for 'ci-runner-07' on 'RHEL 10.0' identified 4 minutes ago. The interface also includes filters for 'Name' and pagination controls.

Red Hat Satellite NB Satellite LabVM Admin User

Search and go

Monitor >

Content >

Hosts >

Red Hat Lightspeed >

Recommendations

Vulnerability

Configure >

Infrastructure >

Administer >

CVE-2026-53362

Actions

Publish date: 21 June 2026

Severity
Important

CVSS 3.0 base score
7.8 Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

A flaw was found in the Linux kernel's ipv6 networking subsystem. An incorrect parameter length calculation allows an attacker with permissions to create UDP sockets to trigger overwrites of kernel memory, potentially leading to privilege escalation, data corruption, or a system crash.

For most up-to-date information, [View in Red Hat CVE database](#)

Filter by name

Name	OS	Last seen
ci-runner-07	RHEL 10.0	4 minutes ago



Lightspeed on premise

der Abgleich bleibt im Haus

The screenshot displays the Red Hat Satellite Lightspeed on premise web interface. The top navigation bar includes the Red Hat Satellite logo, 'NB Satellite', 'LabVM', a notification bell, and the user 'Admin User'. The left sidebar contains a search bar and a menu with options: Monitor, Content, Hosts, Red Hat Lightspeed (expanded), Recommendations (selected), Vulnerability, Configure, Infrastructure, and Administer. The main content area is titled 'Recommendations' and features three summary cards: 'Incidents' (0), 'Critical recommendations' (0), and 'Important recommendations' (1). Below these cards is a filter section with a dropdown for 'Name', a search input 'Filter by name', and filter tags for 'Systems impacted' (1 or more) and 'Status' (Enabled). A 'Reset filters' link is also present. The recommendations table has columns for Name, Modified, Category, Total risk, Systems, and Remediation type. One recommendation is listed: 'A newer version of kernel is installed, but not used. Bug fixes issued by this new kernel version are not applied', modified 3 years ago, categorized under 'Stability', with a total risk of 'Important' and 1 system impacted. The remediation type is 'Playbook'. The bottom of the interface shows pagination: '1-1 of 1' and '1 of 1'.

Red Hat Satellite NB Satellite LabVM Admin User

Search and go

Monitor >

Content >

Hosts >

Red Hat Lightspeed ▾

Recommendations

Vulnerability

Configure >

Infrastructure >

Administer >

Recommendations ⓘ

Incidents ⓘ

Incident 0

Critical recommendations

Critical 0

Important recommendations

Important 1

Filter by name 🔍

Systems impacted 1 or more ✕ Status Enabled ✕ Reset filters

Name ⌵	Modified ⌵	Category ⌵	Total risk ⌵	Systems ⌵	Remediation type ⌵
> A newer version of kernel is installed, but not used. Bug fixes issued by this new kernel version are not applied	3 years ago	Stability	Important 1	1	Playbook ⋮

1-1 of 1 << < 1 of 1 > >>



Stufe 3

Bewerten, wo auch gescannt wird

- Geschäftsrisiko pro System, einzeln oder in Sammelaktion
- CVE-Status pflegen, z.B. bearbeitet oder begründet zurückgestellt
- Vulnerability-Analyse pro Host ein- und ausschaltbar
- Filter nach Betriebssystemversion, Export nach JSON und CSV
- **Zurückstellen heißt nicht immer dasselbe:**
 - Will not fix
 - Fix deferred
 - Out of support scope

Eine Ausnahme ohne Wiedervorlage ist keine Entscheidung, sondern eine Verjährung.



Stufe 4

Am Kernel-Fall: Fix, Neustart, Nachweis

1

Fix ausrollen

Das Erratum kommt per neuer Content-View-Version in die Umgebung und wird per Remote Execution installiert.

Apply RHSA-2026:34911

One or more of the selected Errata are not Installable via your published Content View versions running on the selected hosts. The new Content View Versions (specified below) will be created which will make this Errata Installable in the host's Environment. This new version will replace the current version in your host's Lifecycle Environment. To install these errata immediately on hosts after publishing check the box below.

Content View	Version	Environment	Host Count
rhel10	2.1	dev	1

2

Neustart per Playbook

Advisor erkennt: neuer Kernel installiert, aber nicht aktiv. Für diese Empfehlung gibt es ein Playbook.

Name	Modified	Category	Total risk	Systems	Remediation type
A newer version of kernel is installed, but not used. Bug fixes issued by this new kernel version are not applied	3 years ago	Stability	Important	1	Playbook

3

Erneuter Abgleich

Nach dem Neustart verschwindet ci-runner-07 aus der Liste betroffener Systeme. Das ist der Nachweis.

Name	OS	Last seen
ci-runner-07	RHEL 10.0	4 minutes ago

vorher: ci-runner-07 betroffen → nach dem Neustart: **0 Systeme**

On premise gibt es Playbooks für Advisor-Empfehlungen. Die Cloud-Variante erzeugt sie auch direkt aus dem CVE-Befund.



Patchen automatisieren, ohne die Kontrolle abzugeben

Lässt sich gut automatisieren

- Erhebung, Abgleich, Errata-Rollout
- Erneuter Abgleich als Nachweis
- Rollout über Lifecycle-Umgebungen: Test vor Produktion, mit demselben Content

Bleibt eine Entscheidung

- Wartungsfenster und Neustart
- Welche Systeme in welcher Reihenfolge
- Was passiert, wenn es schiefgeht



Was euch die Automatisierung nicht abnimmt

Kein Werkzeug findet, was es nicht kennt.

Sieht das Werkzeug

RPM-Pakete aus den Repositories

Sieht es nicht

selbst gebaute Software
pip, npm, Go-Module
Appliances
Fremdsoftware ohne VEX
alles, was nicht im Inventar steht

IM GETRENNTEN BETRIEB

cvemap.xml (inzwischen ~373 MB, wächst stetig) kommt von Hand auf den Satellite.

Regelmäßig einspielen, z. B. mit dem Patchzyklus.

Eine alte Datei liefert keine Fehlermeldung, sondern ein sauberes Dashboard mit alten Befunden.



NIS2 und CRA

Zwei EU-Regeln, zwei Rollen

	NIS2 eure Pflicht als Betreiber	CRA die Pflicht eurer Lieferanten
Wer	Mittlere und große Einrichtungen in 18 Sektoren, in Deutschland über 29.000	Hersteller von Produkten mit digitalen Elementen auf dem EU-Markt
Seit wann	In Deutschland seit 06.12.2025 (neues BSIG)	Meldepflichten seit 11.09.2026, alles Weitere ab 11.12.2027
Schwachstellen	Risikomanagement nach § 30 BSIG, u. a. Schwachstellenmanagement und Lieferkette	Schwachstellen im Produkt behandeln, Sicherheitsupdates im Supportzeitraum, SBOM
Melden, wenn	ein erheblicher Sicherheitsvorfall bei euch passiert → BSI	eine Schwachstelle im Produkt aktiv ausgenutzt wird → ENISA
Fristen	24 h · 72 h · 1 Monat	24 h · 72 h · 14 Tage nach verfügbarem Fix

NIS2 verlangt von euch Schwachstellenmanagement. Der CRA verpflichtet eure Lieferanten, die Daten dafür zu liefern.



Was ihr von Lieferanten braucht

Fünf Fragen:

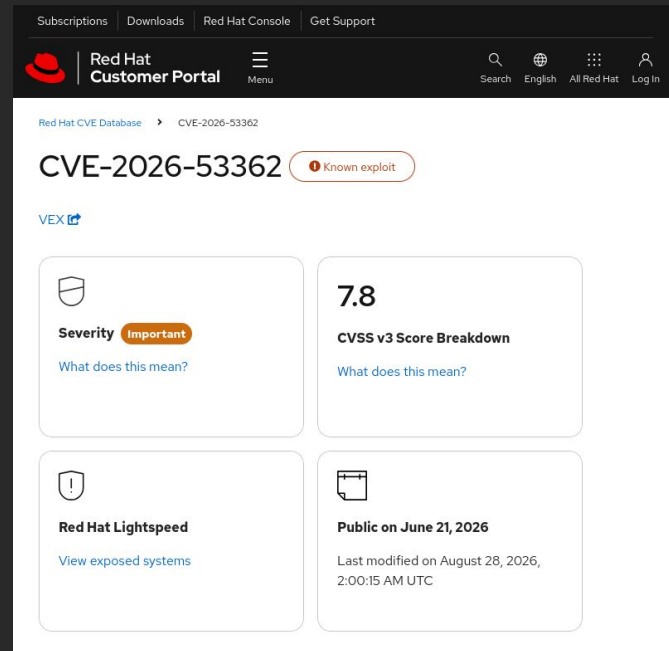
- ▶ Produkt und Version eindeutig identifizierbar?
- ▶ Aktuelle Betroffenheitsaussage mit Begründung?
- ▶ Maschinenlesbare Daten mit dokumentierter Bedeutung?
- ▶ Supportumfang, Updates und Sicherheitskontakt klar?
- ▶ Korrekturen und Statusänderungen nachvollziehbar?

Alles, was diese Fragen nicht beantwortet, bleibt Handarbeit.



Was machen wir damit?

- ▶ CVE-2026-53362 „IPV6_FRAG_ESCAPE“ im Linux-Kernel
- ▶ Lokale Rechteausweitung
- ▶ Container Escape
- ▶ Severity: Important



The screenshot shows the Red Hat Customer Portal interface for CVE-2026-53362. The page includes a navigation bar with links for Subscriptions, Downloads, Red Hat Console, and Get Support. The main header features the Red Hat logo, the text 'Red Hat Customer Portal', a menu icon, and search, language, and login options. The breadcrumb trail indicates the path: Red Hat CVE Database > CVE-2026-53362. The title 'CVE-2026-53362' is prominently displayed with a 'Known exploit' badge. Below the title, there is a 'VEX' link. The page is divided into four informational cards: 1. Severity: Important (with a shield icon and a link to 'What does this mean?'). 2. CVSS v3 Score Breakdown: 7.8 (with a link to 'What does this mean?'). 3. Red Hat Lightspeed (with a shield icon and a link to 'View exposed systems'). 4. Public on June 21, 2026 (with a document icon and the last modified date: August 28, 2026, 2:00:15 AM UTC).



Die Lage in 3 Sätzen:

Die Menge wächst schneller, als man sie von Hand bewerten kann.

Keine Quelle sagt allein, was bei euch kaputt ist.

Werkzeuge nehmen den Abgleich ab, die Entscheidung nicht.



Vielen Dank für die Aufmerksamkeit!

Und wie sieht es bei euch aus?

- Wie oft habt ihr Fehlalarme wegen Backports, wie geht ihr damit um?
- Wer entscheidet bei euch, wann ein Schwachstellen-Ticket wirklich zu ist?
- Wie viel Automatisierung habt ihr schon beim Patchen?
- Hilft euch der CRA im Einkauf, oder ist er vor allem mehr Papier?



linkedin.com/company/red-hat



youtube.com/@redhat



facebook.com/redhat



x.com/RedHat