PRISM DEMO · SECURITY

Sicherheitsbericht

Stand 07.09.2026 um 00:39 Uhr

Auswahl: alle offenen Prüfkontexte, ungefiltert.

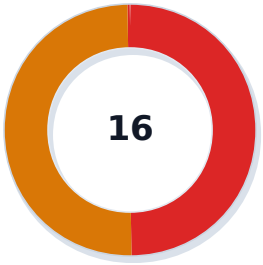
16	8	45	0
OFFENE PRÜFKONTEXTE	KRITISCH ODER HOCH	BETROFFENE SYSTEME	GESCHLOSSEN · LETZTE 90 TAGE

Was sich seit dem letzten Bericht geändert hat

Dies ist der erste erzeugte Bericht. Er legt den Bezugspunkt fest – jeder weitere vergleicht sich gegen den jeweils vorherigen und zeigt an dieser Stelle die Veränderung.

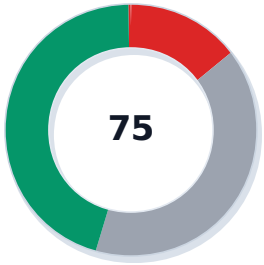
Wie sich die offenen Kontexte verteilen

Nach Schweregrad



- Hoch **8**
- Mittel **8**

Zustand der Systeme



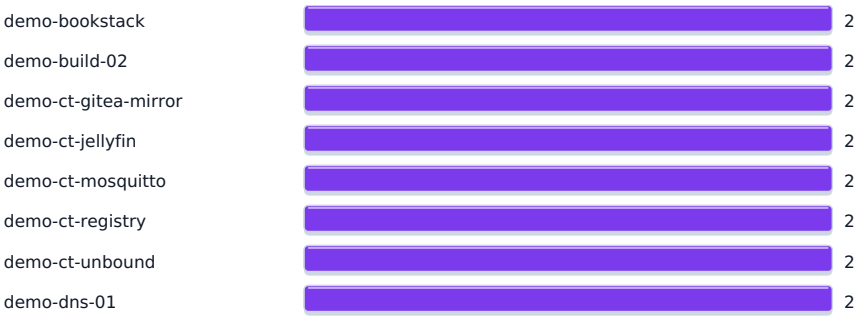
- Sicherheitsupdates verfügbar **11**
- Nicht geprüft **30**
- Keine Sicherheitsupdates **34**

11 von 75 aktiven Systemen haben offene Sicherheitsupdates.

Welche Pakete am meisten Systeme betreffen

Gezählt in Paket-System-Paaren. Oben steht, was mit einer Aktualisierung am meisten auf einmal klärt.

Welche Systeme die meisten offenen Kontexte tragen



Was der Schwachstellenscanner von außen sieht

OpenVAS prüft die Angriffsfläche – erreichbare Dienste statt installierter Pakete. Nur ein Fund, der jede Stufe erreicht, darf eine CVE-Entscheidung automatisch bestätigen.

135
aktuelle Funde

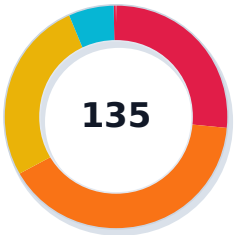
90 mit CVE-Bezug · 45 reine Expositionsbefunde

135
Funde auf 45 zugeordneten Systemen

45
offene oder untersuchte Angriffsflächen

0
gleiches Asset und gleiche Wazuh-CVE

0
nach QoD-Regel automatisch bestätigt



Schweregrad der Außensicht

- Kritisch **36**
- Hoch **54**
- Mittel **36**
- Niedrig **9**

0 Expositionsbefunde sind behoben oder akzeptiert; 0 Funde sind noch keinem Asset zugeordnet.

Derzeit stimmt kein Scannerfund auf demselben System mit derselben Wazuh-CVE überein. Der Scanner verändert deshalb keine CVE-Entscheidung – er ergänzt die Sicht, ersetzt sie nicht.

Priorisierte OpenVAS-Beobachtungen

Spring Framework: Data-Binding-Schwachstelle
CVSS 9,8 · 198.51.100.150:8443/tcp · demo-backup-01 · QoD 80 %
CVE: CVE-2022-22965
Empfohlene Maßnahme: Paket aktualisieren und Dienst neu starten.

Spring Framework: Data-Binding-Schwachstelle
CVSS 9,8 · 198.51.100.20:8443/tcp · demo-ct-gitea-mirror · QoD 80 %
CVE: CVE-2022-22965
Empfohlene Maßnahme: Paket aktualisieren und Dienst neu starten.

Spring Framework: Data-Binding-Schwachstelle
CVSS 9,8 · 198.51.100.12:8443/tcp · demo-ct-paperless · QoD 80 %
CVE: CVE-2022-22965
Empfohlene Maßnahme: Paket aktualisieren und Dienst neu starten.

Spring Framework: Data-Binding-Schwachstelle
CVSS 9,8 · 198.51.100.123:8443/tcp · demo-dns-01 · QoD 80 %
CVE: CVE-2022-22965
Empfohlene Maßnahme: Paket aktualisieren und Dienst neu starten.

Spring Framework: Data-Binding-Schwachstelle

CVSS 9,8 · 198.51.100.118:8443/tcp · demo-grafana · QoD 80 %
CVE: CVE-2022-22965

Empfohlene Maßnahme: Paket aktualisieren und Dienst neu starten.

Die dringendsten Einzelfälle

Sortiert nach Schweregrad und Verbreitung. Die vollständige Liste steht in PRISM und im CSV-Export – acht Seiten Tabelle liest niemand.

SCHWERE	CVE	PAKET	SYSTEME	WARUM OFFEN
High	CVE-2021-4034	policykit-1 0.105-33	**17** demo-bookstack, demo-build-02, demo-ct-gitea-mirror, demo-ct-jellyfin, demo-ct-mosquitto, demo-ct-registry, demo-ct-unbound, demo-dns-01, demo-docker-01, demo-gitlab, demo-greenbone, demo-keycloak, demo-mail, demo-openbao, demo-prometheus, demo-proxy-02, demo-test-web	Noch kein Evidenz-Audit gelaufen
High	CVE-2023-4863	libwebp7 1.2.4-0.2	**17** demo-bookstack, demo-build-02, demo-ct-gitea-mirror, demo-ct-jellyfin, demo-ct-mosquitto, demo-ct-registry, demo-ct-unbound, demo-dns-01, demo-docker-01, demo-gitlab, demo-greenbone, demo-keycloak, demo-mail, demo-openbao, demo-prometheus, demo-proxy-02, demo-test-web	Noch kein Evidenz-Audit gelaufen
Medium	CVE-2021-44228	log4j-core 2.14.1	**16** demo-backup-01, demo-build-01, demo-checkmk, demo-ct-homeassistant, demo-ct-minio, demo-ct-paperless, demo-ct-syslog, demo-ct-uptime, demo-dns-02, demo-docker-02, demo-grafana, demo-jump-01, demo-ldap-01, demo-nas-01, demo-pbs-01, demo-proxy-01	Noch kein Evidenz-Audit gelaufen
Medium	CVE-2022-22965	spring-beans 5.3.20	**16** demo-backup-01, demo-build-01, demo-checkmk, demo-ct-homeassistant, demo-ct-minio, demo-ct-paperless, demo-ct-syslog, demo-ct-uptime, demo-dns-02, demo-docker-02, demo-grafana, demo-jump-01, demo-ldap-01, demo-nas-01, demo-pbs-01, demo-proxy-01	Noch kein Evidenz-Audit gelaufen
High	CVE-2021-4034	policykit-1 0.105-33	**4** demo-k8s-cp-01, demo-k8s-worker-02, demo-nextcloud, demo-wazuh	Noch kein Evidenz-Audit gelaufen
High	CVE-2023-4863	libwebp7 1.2.4-0.2	**4** demo-k8s-cp-01, demo-k8s-worker-02, demo-nextcloud, demo-wazuh	Noch kein Evidenz-Audit gelaufen
Medium	CVE-2021-44228	log4j-core 2.14.1	**3** demo-k8s-worker-01, demo-k8s-worker-03, demo-rancher	Noch kein Evidenz-Audit gelaufen

SCHWERE	CVE	PAKET	SYSTEME	WARUM OFFEN
Medium	CVE-2022-22965	spring-beans 5.3.20	**3** demo-k8s-worker-01, demo-k8s-worker-03, demo-rancher	Noch kein Evidenz-Audit gelaufen
Medium	CVE-2021-44228	log4j-core 2.14.1	**2** demo-node-01, demo-node-03	Noch kein Evidenz-Audit gelaufen
Medium	CVE-2022-22965	spring-beans 5.3.20	**2** demo-node-01, demo-node-03	Noch kein Evidenz-Audit gelaufen
High	CVE-2021-4034	policykit-1 0.105-33	**1** demo-awx	Noch kein Evidenz-Audit gelaufen
High	CVE-2021-4034	policykit-1 0.105-33	**1** demo-node-02	Noch kein Evidenz-Audit gelaufen
High	CVE-2023-4863	libwebp7 1.2.4-0.2	**1** demo-awx	Noch kein Evidenz-Audit gelaufen
High	CVE-2023-4863	libwebp7 1.2.4-0.2	**1** demo-node-02	Noch kein Evidenz-Audit gelaufen
Medium	CVE-2021-44228	log4j-core 2.14.1	**1** demo-vaultwarden	Noch kein Evidenz-Audit gelaufen
Medium	CVE-2022-22965	spring-beans 5.3.20	**1** demo-vaultwarden	Noch kein Evidenz-Audit gelaufen