SUSE Live Patching aktivieren

04.11.2026 00:55:12

FAQ-Artikel-Ausdruck

Kategorie:	Server-Dienste	**Bewertungen:**	0
Status:	öffentlich (Alle)	**Ergebnis:**	0.00 %
Sprache:	de	**Letzte Aktualisierung:**	14:54:08 - 03.11.2026

Schlüsselwörter

suse,sles,livepatch,live,patch

Lösung (öffentlich)

Mit SUSE Live Patching stellt SUSE ausgewählte Sicherheitsupdates für den Linux-Kernel und unterstützte Systembibliotheken früher bereit als über den regulären Update-Kanal. Diese können im laufenden Betrieb eingespielt werden, ohne dass dafür ein Neustart des Systems bzw. der betroffenen Anwendungen erforderlich ist.

Unter SLES 15 SP7 werden zwei Arten von Live Patching unterstützt:

- Kernel Live Patching (KLP): Aktualisierung des laufenden Linux-Kernels.

- User Space Live Patching (ULP): Aktualisierung unterstützter Systembibliotheken wie glibc und OpenSSL in laufenden Anwendungen.

Die folgende Anleitung beschreibt die Aktivierung unter SUSE Linux Enterprise Server 15 SP7:

- Live-Patching-Modul registrieren

Die Registrierung des Live-Patching-Moduls ist Voraussetzung für KLP und ULP.

SUSEConnect -p sle-module-live-patching/15.7/x86_64

Registriert das Modul SUSE Linux Enterprise Live Patching 15 SP7 über den konfigurierten RMT-Server.

Anschließend die Paketquellen aktualisieren:

zypper refresh

- Kernel Live Patching (KLP) aktivieren

Installieren Sie das Pattern lp_sles einschließlich der benötigten Komponenten und Abhängigkeiten:

zypper install -t pattern lp_sles

Damit wird Kernel Live Patching aktiviert. Ein verfügbarer initialer Live-Patch für den aktuell laufenden Kernel wird dabei ebenfalls installiert und angewendet.

Status überprüfen

Mit folgenden Befehlen lässt sich der Status des Kernel Live Patchings überprüfen:

klp status

Zeigt den aktuellen Status des Kernel Live Patchings.

klp -v patches

Zeigt die installierten und aktiven Kernel-Live-Patches einschließlich der behobenen Fehler und CVEs.

zypper se --details kernel-livepatch-*

Zeigt die installierten Kernel-Live-Patching-Pakete.

Hinweis: Die Ausgabe von uname -r ändert sich durch das Einspielen eines Live-Patches nicht. Reguläre Kernel-Updates bleiben weiterhin erforderlich und können einen Neustart notwendig machen.

- User Space Live Patching (ULP) aktivieren

Für User Space Live Patching müssen zunächst die benötigten Komponenten installiert werden:

zypper install libpulp0 libpulp-tools

SUSE stellt Live-Patches für folgende Systembibliotheken bereit:

- glibc
- OpenSSL 1.1
- OpenSSL 3

Installieren Sie die entsprechenden Live-Patching-Pakete:

zypper install glibc-livepatches openssl-1_1-livepatches openssl-3-livepatches

Damit eine Anwendung Live-Patches für ihre Bibliotheken verwenden kann, muss sie mit der Bibliothek libpulp.so.0 gestartet werden. Dies erfolgt beispielsweise über:

LD_PRELOAD=/usr/lib64/libpulp.so.0 APPLICATION_CMD

Ersetzen Sie APPLICATION_CMD durch den entsprechenden Anwendungsaufruf.

Status überprüfen

Mit folgendem Befehl lässt sich überprüfen, auf welche laufenden Anwendungen Live-Patches angewendet wurden:

ulp patches

Die Ausgabe zeigt die betroffenen Prozesse, die live-patchbaren Bibliotheken und die angewendeten Patches einschließlich der behobenen Fehler.

Live-Patches werden im Rahmen der regulären Systemupdates bereitgestellt und installiert, sofern die entsprechenden Live-Patching-Pakete installiert sind.
Live Patching ersetzt keine regulären System- und Kernel-Updates. Nicht alle Sicherheitskorrekturen können als Live-Patch bereitgestellt werden. Reguläre Updates und gegebenenfalls erforderliche Neustarts müssen daher weiterhin durchgeführt werden.

Weitere Informationen:

-

[1]SUSE-Dokumentation: Kernel Live Patching (KLP)

-

[2]SUSE-Dokumentation: User Space Live Patching (ULP)

[1] https://documentation.suse.com/sles/15-SP7/html/SLES-all/cha-klp.html
[2] https://documentation.suse.com/sles/15-SP7/html/SLES-all/cha-ulp.html