



Informacje o wydaniu

openSUSE Leap to darmowy system operacyjny oparty na Linuksie dla komputera PC, laptopa lub serwera. Możesz surfować po Internecie, zarządzać wiadomościami e-mail i zdjęciami, wykonywać pracę biurową, odtwarzać filmy lub muzykę i świetnie się bawić!

Data wydania: 2022-12-31, : 15.3.20221231.096cd3b

Spis treści

- 1 Instalacja 2
- 2 Aktualizacja systemu 6
- 3 Usunięte i przestarzałe pakiety i funkcje 8
- 4 Drivers and hardware 10
- 5 Pulpit 11
- 6 More information and feedback 11

Informacje o wydaniu są nieustannie aktualizowane. Aby sprawdzić najnowszą wersję, sprawdź <https://doc.opensuse.org/release-notes>. Angielska wersja jest aktualizowana na bieżąco. Tłumaczenia natomiast mogą być tymczasowo nieaktualne.

Jeśli openSUSE jest aktualizowane ze starszej wersji, zobacz wcześniejsze informacje o wydaniu zamieszczone na: https://en.opensuse.org/openSUSE:Release_Notes.

Informacje o projekcie znajdują się na stronie <https://www.opensuse.org>.

Do zgłaszania problemów z tą wersją, skorzystaj z Bugzilli openSUSE. W celu uzyskania dodatkowych informacji odwiedź https://en.opensuse.org/Submitting_Bug_Reports.

Najważniejsze nowe funkcje openSUSE Leap 15.3 są również wymienione pod adresem https://en.opensuse.org/Features_15.3.

1 Instalacja

Ta sekcja zawiera uwagi dotyczące instalacji. Szczegółowe instrukcje instalacji można znaleźć w dokumentacji pod adresem <https://doc.opensuse.org/documentation/leap/startup/html/book-startup/part-basics.html>.

1.1 openSUSE Leap now has three update repositories

Konfiguracja konserwacyjna openSUSE Leap 15.3 składa się z trzech głównych repozytoriów aktualizacji. Są to: repo-update, repo-backports-update i repo-sle-update. Dwa ostatnie są nowe i są wynikiem ponownego wykorzystania plików binarnych z SUSE Linux Enterprise. Te repozytoria są dostępne i sprawdzane podczas instalacji online openSUSE Leap. Zalecamy ich używanie. Nowe definicje repozytoriów aktualizacji dla openSUSE Leap 15.3 będą dodatkowo dostarczane przez 0-dniową aktualizację konserwacyjną pakietu openSUSE-release. Aktualizacja zostanie dostarczona za pośrednictwem tradycyjnego kanału konserwacji repo-update. Będzie nosił specjalną flagę aktualizacji, co oznacza, że dotyczy obszaru zarządzania oprogramowaniem, który jest następnie specjalnie obsługiwany przez zypper. Powinieneś dwukrotnie sprawdzić za pomocą polecenia **zypper up**, czy wszystkie aktualizacje zostały przetworzone. Aby uzyskać więcej informacji, zobacz https://bugzilla.opensuse.org/show_bug.cgi?id=1186593.

Repozytorium repo-update służy do aktualizacji openSUSE Leap (OSS). Jest to najmniejszy i zawiera pakiety konfiguracji systemu, w tym pakiet wersji, branding i potencjalne rozwidlenia pakietów SUSE Linux Enterprise. To repozytorium ma również wariant debug-info.

The `repo-backports-update` repository is an update repository for openSUSE Backports that contains updates for the majority of openSUSE Leap packages. This repository also has a `debug-info` variant.

Trzecie repozytorium, nazwane `repo-sle-update`, jest repozytorium aktualizacji, które zawiera połączone aktualizacje ze wszystkich aktywnych strumieni aktualizacji SUSE Linux Enterprise. To repozytorium nie zawiera wariantu `debug-info`.

1.2 Korzystanie z aktualizacji atomowych z rolą systemową *Serwer transakcyjny*

Instalator obsługuje rolę systemową *Serwer transakcyjny*. Ta rola systemowa obejmuje system aktualizacji, który stosuje aktualizacje niepodzielnie (jako pojedynczą operację) i ułatwia ich przywrócenie, jeśli zajdzie taka potrzeba. Funkcje te są oparte na narzędziach do zarządzania pakietami, na których opierają się również wszystkie inne dystrybucje SUSE i openSUSE. Oznacza to, że zdecydowana większość pakietów RPM, które współpracują z innymi rolami systemowymi openSUSE Leap 15.3, działa również z rolą systemową *Serwer transakcyjny*.



Uwaga: Niekompatybilne pakiety

Niektóre pakiety modyfikują zawartość `/var` lub `/srv` w swoich skryptach RPM `%post`. Te pakiety są niezgodne. Jeśli znajdziesz taki pakiet, zgłoś błąd.

Aby zapewnić te funkcje, ten system aktualizacji opiera się na:

- **Migawki Btrfs.** Przed rozpoczęciem aktualizacji systemu tworzona jest nowa migawka Btrfs głównego systemu plików. Następnie wszystkie zmiany z aktualizacji są instalowane w tej migawce Btrfs. Aby zakończyć aktualizację, możesz ponownie uruchomić system w nowej migawce.
Aby cofnąć aktualizację, po prostu uruchom komputer z poprzedniej migawki.
- **Główny system plików tylko do odczytu.** Aby uniknąć problemów i utraty danych z powodu aktualizacji, główny system plików nie może być zapisany w inny sposób. Dlatego podczas normalnej pracy główny system plików jest montowany tylko do odczytu.
Aby ta konfiguracja działała, należy wprowadzić dwie dodatkowe zmiany w systemie plików: Aby umożliwić zapisywanie konfiguracji użytkownika w `/etc`, ten katalog jest automatycznie konfigurowany do używania OverlayFS. `/var` jest teraz oddzielnym podwoluminem, do którego mogą zapisywać procesy.

! Ważne: Serwer transakcyjny potrzebuje co najmniej 12 GB miejsca na dysku

Rola systemowa *Serwer transakcyjny* wymaga dysku o rozmiarze co najmniej 12 GB, aby pomieścić migawki Btrfs.

! Ważne: YaST nie działa w trybie transakcyjnym

Obecnie YaST nie działa z aktualizacjami transakcyjnymi. Dzieje się tak dlatego, że YaST wykonuje rzeczy natychmiast i ponieważ nie może edytować systemu plików tylko do odczytu.

Aby pracować z aktualizacjami transakcyjnymi, zawsze używaj polecenia **transactional-update** zamiast YaST i Zypper do zarządzania całym oprogramowaniem:

- Zaktualizuj system: **transactional-update up**
- Zainstaluj pakiet: **pkg aktualizacji transakcyjnej w NAZWA_PAKIETU**
- Usuń pakiet: **transactional-update pkg rm PACKAGE_NAME**
- Aby przywrócić ostatnią migawkę, czyli ostatni zestaw zmian w głównym systemie plików, upewnij się, że system jest uruchomiony w przedostatnim migawce i uruchom: **transactional-update rollback**
Opcjonalnie dodaj identyfikator migawki na końcu polecenia, aby przywrócić określony identyfikator.

W przypadku korzystania z tej roli systemowej system domyślnie przeprowadza codzienną aktualizację i uruchamia się ponownie między 03:30 a 05:00. Obie te akcje są oparte na systemie i w razie potrzeby można je wyłączyć za pomocą **systemctl**:

```
systemctl disable --now transactional-update.timer rebootmgr.service (PL)
```

Aby uzyskać więcej informacji o aktualizacjach transakcyjnych, zobacz posty na blogu openSUSE Kubic <https://kubic.opensuse.org/blog/2018-04-04-transactionalupdates/> i <https://kubic.opensuse.org/blog/2018-04-20-transactionalupdates2/>.

1.3 Instalacja na dyskach twardych o pojemności mniejszej niż 12 GB

Instalator zaproponuje schemat partycjonowania tylko wtedy, gdy dostępny rozmiar dysku twardego jest większy niż 12 GB. Jeśli chcesz skonfigurować na przykład bardzo małe obrazy maszyn wirtualnych, użyj partycjonera z przewodnikiem, aby ręcznie dostosować parametry partycjonowania.

1.4 UEFI — zunifikowany, rozszerzalny interfejs oprogramowania układowego

Przed zainstalowaniem openSUSE w systemie, który uruchamia się za pomocą UEFI (Unified Extensible Firmware Interface), pilnie zaleca się sprawdzenie wszelkich aktualizacji oprogramowania sprzętowego zalecanych przez dostawcę sprzętu i, jeśli są dostępne, zainstalowanie takiej aktualizacji. Wstępna instalacja systemu Windows 8 lub nowszego wyraźnie wskazuje, że system uruchamia się przy użyciu UEFI.

Wyjaśnienie: Zdarza się, że firmware interfejsu UEFI zawiera błędy, które powodują niepoprawne działanie, gdy zbyt duża ilość danych jest zapisywana w buforze UEFI. Nie wiadomo jak dużo to „za dużo”.

openSUSE ogranicza ryzyko zapisania większej ilości danych niż jest to niezbędne. Wskazane jest wyłącznie położenie menadżera rozruchu openSUSE. Jądro Linux zapewnia możliwość użycia bufora UEFI do zapisywania informacji dotyczących uruchamiania i błędów, jednakże funkcja (`pstore`) domyślnie jest zablokowana. Niezależnie od tego zaleca się instalowanie aktualizacji firmware polecanych przez producenta sprzętu.

1.5 Partycje UEFI, GPT i MS-DOS

Wraz ze specyfikacją EFI/UEFI pojawił się nowy styl partycjonowania: GPT (Tabela partycji GUID). Ten nowy schemat używa globalnie unikatowych identyfikatorów (wartości 128-bitowe wyświetlane w 32 cyfrach szesnastkowych) do identyfikacji urządzeń i typów partycji.

Dodatkowo, specyfikacja UEFI partycje MRB (MS-DOS) są kompatybilne wstecz. Program rozruchowy LINUX (ELILO lub GRUB2) próbuje automatycznie wygenerować GUID dla tych partycji i zapisuje je w firmwarze. Takie GUID mogą się często zmieniać, wywołując nadpisanie w firmwarze. Na nadpisanie składają się dwie operacje: Usunięcie starego wpisu oraz stworzenie nowego który zastępuje pierwszy.

Nowoczesny firmware posiada kolektor śmieci który zbiera usunięte wpisy i uwalnia pamięć zarezerwowaną dla starego wpisu. Problem powstaje gdy wadliwy firmware nie zbiera i uwalnia tych wpisów. Może to doprowadzić do problemów z uruchomieniem systemu.

W celu ominięcia problemu, przekształć stare partycje MRB na GPT.

1.6 tlp package service

During installation on a laptop, the `tlp` package is installed (together with its sub-package `tlp-rdw`, if the installation of recommended packages is enabled). This package provides additional tools to save battery power on laptops, especially Lenovo laptops.

The service is not enabled by default because it might interfere with other specialized laptop tools, for example, `laptop-mode-tools`, `rftkill`, `gnome-power-manager`, or `kde-power-manager`. To enable and start the service explicitly, use YaST Services Manager or use the command `systemctl enable --now tlp.service`. If you encounter any unexpected behavior afterward, for example, WiFi problems or non-functional USB ports, disable the service again.

2 Aktualizacja systemu

Ta sekcja zawiera uwagi dotyczące aktualizacji systemu. Obsługiwane scenariusze i szczegółowe instrukcje uaktualniania można znaleźć w dokumentacji pod adresem:

- https://en.opensuse.org/SDB:System_upgrade ↗
- <https://doc.opensuse.org/documentation/leap/startup/html/book-startup/cha-update-osuse.html> ↗

Dodatkowo sprawdź *Sekcja 3, „Usunięte i przestarzałe pakiety i funkcje”*.

2.1 Bezproblemowa aktualizacja z openSUSE Leap 15.2

openSUSE Leap 15.3 jest nowo zbudowany na binarnych pakietach RPM z SUSE Linux Enterprise Server. Ta zmiana została wprowadzona w ramach starań Closing The Leap Gap (CtLG) mających na celu zbliżenie do siebie openSUSE Leap i SUSE Linux Enterprise Server.

W przeciwieństwie do 15.2, domyślna instalacja openSUSE Leap 15.3 zawiera większość RPM z SUSE Linux Enterprise Server. Te RPM są podpisane przez SUSE LLC zamiast używania klucza openSUSE. Pakiet `libzypp` w wersji 12.25.8 wprowadził białą listę dla wymiany dostawców SUSE LLC i openSUSE, aby umożliwić bezproblemową migrację. Ta biała lista eliminuje potrzebę określenia `--allow-vendor-change` tylko dla wymiany dostawców openSUSE i SUSE LLC. Nadal może być konieczne określenie `--allow-vendor-change` podczas migracji, jeśli używasz repozytoriów OBS podpisanych innymi kluczami.

openSUSE Leap releases older than 15.2 do not contain this feature because they are not supported anymore. All users are advised to upgrade to openSUSE Leap 15.2 with the latest updates before upgrading to 15.3. The following parameters can be used as a workaround for `libzypp` versions older than 12.25.8 (replace 15.0 below with your current openSUSE version):

```
zypper addrepo --check --refresh --name 'openSUSE-Leap-15.0-Update' http://
download.opensuse.org/update/leap/15.0/oss/ repo-update
zypper dup --allow-vendor-change --force-resolution
```

openSUSE Leap 15.3 zapewnia wszystkie wymagane klucze weryfikacji RPM, w tym klucze SUSE Linux Enterprise Server, jako część pakietu `openSUSE-build-key`. Wszystkie klucze są również nowo dostępne w repozytorium OSS.

Pakiet `libzypp` w wersji 17.25.11 powinien automatycznie importować wymagane klucze, które są identyfikowane jako zaufane. Jeśli tak, zostaniesz powiadomiony o imporcie i żadne inne działania nie będą potrzebne.

Jeśli system nie zaimportował klucza, który został użyty do podpisania `repodata`, będziesz musiał zaimportować go ręcznie. Możesz to sprawdzić, uruchamiając następujące polecenie:

```
rpm -qa gpg- pubkey
```

Dane wyjściowe powinny zawierać wiersz rozpoczynający się następującym tekstem: `gpg-pubkey-39db7c82-*`. Jeśli tak nie jest, wykonaj następujące czynności, aby ręcznie zaimportować klucz:

- Pobierz klucz SUSE Linux Enterprise 15 z <https://download.opensuse.org/distribution/leap/15.3/repo/oss/gpg-pubkey-39db7c82-5847eb1f.asc>.
- Zapisz klucz w katalogu `/var/cache/zypp/pubkeys`. Zmień jego nazwę tak, aby kończyła się na `.key`.
- Uruchom polecenie `zypper dup`. Zostaniesz poproszony o zaimportowanie brakującego klucza. Stanie się tak, nawet jeśli klucz znajduje się w katalogu wspomnianym powyżej. Jeśli plik zawiera wiele kluczy, `zypper` zaimportuje tylko wymagany klucz.

Aby uzyskać więcej informacji, zobacz https://bugzilla.opensuse.org/show_bug.cgi?id=1184326.

2.2 Dopasowanie pakietów jądra SUSE Linux Enterprise Server i openSUSE Leap

On openSUSE Leap, the default kernel has been split into three subpackages: `kernel-default`, `kernel-default-extra`, and `kernel-default-optional`. Similarly, `kernel-preempt` has also been split into `kernel-preempt`, `kernel-preempt-extra`, and `kernel-preempt-optional`. The `-optional` package contains optional modules only for openSUSE Leap. The `-extra` package contains unsupported modules. The kernel preemption mode can be controlled by setting the `preempt=voluntary` kernel parameter on the command line. This parameter works with `kernel-default`.

Jeśli używasz tego wariantu jądra, upewnij się, że wszystkie pakiety RPM wymagane dla twojego przypadku użycia są zainstalowane.

3 Usunięte i przestarzałe pakiety i funkcje

3.1 Przestarzałe pakiety i funkcje

Przestarzałe pakiety są nadal dostarczane jako część dystrybucji, ale planowane jest ich usunięcie w następnej wersji openSUSE Leap. Pakiety te istnieją w celu ułatwienia migracji, ale ich użycie jest odradzane i mogą nie otrzymywać aktualizacji.

- `midori`, lekka przeglądarka internetowa oparta na WebKit i GTK+, nie jest już obsługiwana i ma zostać usunięta w następnym wydaniu.

Aby sprawdzić, czy zainstalowane pakiety nie są już obsługiwane: Upewnij się, że `lifecycle-data-openSUSE` jest zainstalowany, a następnie użyj polecenia:

```
cykl życia zypper
```

3.2 Usunięte pakiety i funkcje

Usunięte pakiety nie są już dostarczane jako część dystrybucji.

- libqt4 i kdelibs4 zostały usunięte, ponieważ nie były konserwowane i miały problemy z bezpieczeństwem. Aby uzyskać więcej informacji, zobacz *Sekcja 5.1, „KDE 4 and Qt4 have been removed”*.

3.2.1 Usunięto obsługę ReiserFS

W openSUSE Leap 15.3 obsługa ReiserFS została całkowicie usunięta z YaST i jądra, a instalator zablokuje aktualizację, gdy wykryje system plików ReiserFS.

W przypadku istniejących partycji danych sformatowanych za pomocą ReiserFS, sugerujemy przekonwertowanie ich na Btrfs przed migracją systemu do openSUSE Leap 15.3.

3.2.2 Berkeley DB usunięty z pakietów

Berkeley DB, używany jako baza danych w niektórych pakietach, posiada podwójną licencję na licencji GNU AGPLv3/Sleepycat. Ponieważ dostawcy usług, którzy redystrybuują nasze pakiety, mogą znaleźć pakiety z tymi licencjami potencjalnie szkodliwe dla ich rozwiązań, zdecydowaliśmy się usunąć Berkeley DB jako zależność od tych pakietów. W dłuższej perspektywie firma SUSE ma na celu zapewnienie rozwiązania bez Berkeley DB.

Ta zmiana dotyczy następujących pakietów:

- kwiecień
- cyrus-sasl
- iproute2
- perl
- php7
- postfix
- rpm

4 Drivers and hardware

4.1 Secure Boot: SUSE Linux Enterprise kernel and openSUSE signed Kernel Module Packages

The newly introduced `openSUSE-signkey-cert` package is required for openSUSE KMPs like `virtualbox`, but only in Secure Boot mode. The package includes the certificate of openSUSE signing key for signing kernel module file (`.ko`) in openSUSE KMP and calls `mokutil` to help user enroll the certificate to MOK. This way, the openSUSE KMP can be verified by the kernel.

If you do not have the base pattern installed and are using any of these KMPs, we recommend installing the `openSUSE-signkey-cert` package manually. A system reboot is required. More information about this process and manual enrollment can be found at https://en.opensuse.org/SDB:NVIDIA_drivers#Secureboot.

4.2 Secure Boot: third-party drivers need to be properly signed

openSUSE Leap 15.2 and later enable a kernel module signature check for third-party drivers (`CONFIG_MODULE_SIG=y`). This is an important security measure to avoid untrusted code running in the kernel.

Może to uniemożliwić ładowanie modułów jądra innych firm, jeśli jest włączony UEFI Secure Boot. Pakiety modułów jądra (KMP) z oficjalnych repozytoriów openSUSE nie są naruszone, ponieważ moduły, które zawierają, są podpisane kluczem openSUSE. Sprawdzanie podpisu ma następujące zachowanie:

- Moduły jądra, które są niepodpisane lub podpisane kluczem, który jest znany jako niezaufany lub którego nie można zweryfikować w bazie danych zaufanych kluczy systemu, zostaną zablokowane.

Możliwe jest wygenerowanie certyfikatu niestandardowego, zarejestrowanie go w bazie danych klucza właściciela komputera (MOK) systemu i podpisanie lokalnie skompilowanych modułów jądra za pomocą klucza tego certyfikatu. Moduły podpisane w ten sposób nie będą blokowane ani nie będą powodować ostrzeżeń. Zobacz <https://en.opensuse.org/openSUSE:UEFI>.

Ponieważ dotyczy to również sterowników graficznych NVIDIA, zajęliśmy się tym w naszych oficjalnych pakietach dla openSUSE. Musisz jednak ręcznie zarejestrować nowy klucz MOK po instalacji, aby nowe pakiety działały. Aby uzyskać instrukcje, jak zainstalować sterowniki i zarejestrować klucz MOK, zobacz https://en.opensuse.org/SDB:NVIDIA_drivers#Secureboot.

5 Pulpit

This section lists desktop issues and changes in openSUSE Leap 15.3.

5.1 KDE 4 and Qt4 have been removed

KDE 4 packages are no longer part of openSUSE Leap 15.3. Update your system to Plasma 5 and Qt 5. Some Qt 4 packages may still remain for compatibility reasons. For more information, see https://bugzilla.opensuse.org/show_bug.cgi?id=1179613.

5.2 Manual config migration of IBus is necessary due to layout name change

Since IBus version 1.5.23 renamed some keyboard layouts, it cannot load configuration containing these renamed layouts after upgrading. Thereby, it might reset the layout to US. Layouts of the following languages are affected: Belgian, German, Greek, Romanian, and Slovak. See https://bugzilla.opensuse.org/show_bug.cgi?id=1177545 for more information.



Users need to migrate configuration manually. Open GNOME Settings and choose an appropriate layout. For desktop environments other than GNOME, run ibus-setup instead.

6 More information and feedback

- Przeczytaj dokumenty README na nośniku.
- Zobacz szczegółowe informacje z dziennika zmian dotyczące konkretnego pakietu z jego RPM:

```
rpm --changelog -qp NAZWA PLIKU.rpm
```

Zastąp FILENAME nazwą RPM.

- Sprawdź plik ChangeLog na najwyższym poziomie nośnika, aby znaleźć chronologiczny dziennik wszystkich zmian dokonanych w zaktualizowanych pakietach.
- Znajdź więcej informacji w katalogu docu na nośniku.
- Aby uzyskać dodatkową lub zaktualizowaną dokumentację, zobacz <https://doc.opensuse.org/> .
- Aby uzyskać najnowsze informacje o produkcie, openSUSE, odwiedź <https://www.opensuse.org> .

Copyright © SUSE LLC