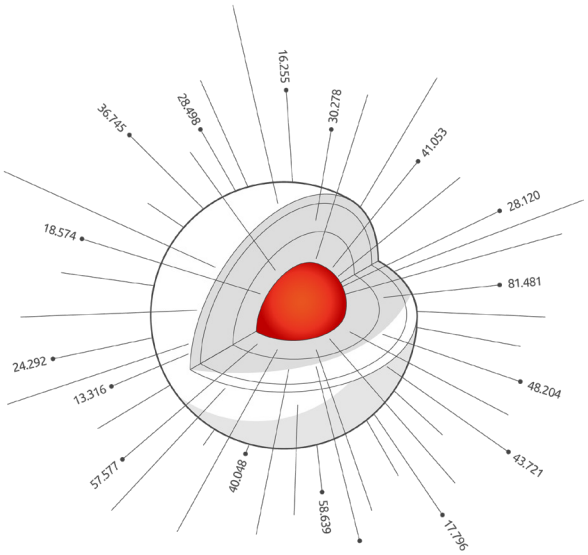

Mitigate Linux kernel exploits with Canonical Livepatch

Security patching automation with rebootless security updates for the Linux kernel. Close exploit windows by patching vulnerabilities without uptime disruptions.

WHAT IS LIVEPATCH?

Livepatch is a security patching automation solution for the Linux kernel, designed to secure your Ubuntu instances against critical or high Common Vulnerabilities and Exposures (CVEs), until the next security patching and reboot window. Livepatch:

- Provides security patching automation for Ubuntu LTS and Ubuntu Core Linux kernels on amd64 and s390x CPU architectures
- Enables incremental roll-outs by allowing system administrators to set a patching cut-off date, and a patching delay, on each machine.
- Is included in Ubuntu Pro

KEY BENEFITS

Added security without downtime

Livepatch provides rebootless kernel patching. It can be applied to running systems, deferring the need to reboot the Ubuntu instance with a patched Linux kernel.

Smaller exploit windows

The Linux kernel is secured against critical and high vulnerabilities between scheduled security maintenance windows. Livepatch eliminates unplanned reboots, and applies available critical and high security patches before any manual security patching intervention occurs. Security patches to vulnerable functions in the Linux kernel are applied in memory, on running systems.

Over a decade of security patches

12 years of security patches for the General Availability (GA) kernel, and the latest Hardware Enablement (HWE) kernel for an Ubuntu LTS release.

Livepatch security coverage windows align with Ubuntu's schedule. The latest version of the kernels available for an Ubuntu LTS release will continue receiving security patches through Livepatch for the duration of an Ubuntu Pro subscription.

Granular control over patch rollout

With awareness of Availability Zones and the ability to enforce the delivery of cumulative security patches to a specific point in time, patch drift is no longer a concern. This capability is available in connected and airgapped environments, with the self-hosted Livepatch Server providing the capability to group machines into tiers, so patch sets can be promoted from one tier to the next.

FEATURES FOR SECURITY, STABILITY, AND CONTROL

Upgrading the kernel package requires rebooting the machine. Instead of upgrading the kernel package, Livepatch applies security fixes to the running kernel in memory. The process to assemble a Livepatch update follows the same regimented process that goes into publishing a kernel package update - just like Ubuntu's Linux kernel packages, the stability and reliability of Canonical's Livepatch updates is extremely high.

With Canonical's Livepatch security patching automation solution, you have full control over which cumulative security patches are applied, when, and where.

Cumulative patching

Uniformly secure against critical and high severity vulnerabilities even in environments with patch drift.

Tiered patch rollout by groups

Ubuntu Pro free tier users are first to receive Livepatch updates. Ubuntu Pro paid users subsequently get Livepatch updates through a phased distribution.

Scheduled and grouped patching

Paid Ubuntu Pro customers can control their own rollouts with controls in either Livepatch Client, or a self-hosted Livepatch Server. Livepatch Client supports cut-off dates, and delays, to ensure groups of machines are consistently and predictably patched.

Deferred reboots

Apply critical and high kernel security fixes in memory without changing the version of the Linux kernel package on disk.

HOW DOES IT WORK?

Kernel live patching inoculates your server while the system is running, without requiring a reboot. canonical-livepatch is a snap package responsible for downloading and inserting live patches. Canonical’s Livepatch solution aligns with the upstream Linux kernel’s live patching technology. Canonical Livepatch compiles a new function which addresses a security vulnerability, and redirects calls to this new, patched function.

Client-server model

Livepatch uses a client-server architecture, where a central Livepatch Server delivers cumulative security patches for the running Linux kernel in Ubuntu LTS or Ubuntu Core. This central Livepatch Server is hosted at livepatch.canonical.com, but Livepatch Server can be self-hosted in network restricted or airgapped environments.

Livepatch Server is optional in network-connected environments, and can be run on-premises or on public cloud. Livepatch Server is available as a self-hosted application, or as a Canonical Managed Application. Canonical's Managed Applications include uptime guarantees through a Service Level Agreement (SLA), and are security patched and upgraded by Canonical.

Livepatch Server is available through a software-as-a-service (SaaS) model at livepatch.canonical.com, and patches are downloaded from livepatch.canonical.com by default. Livepatch Server can be self-hosted on-premises or in a public cloud, and can be deployed on a single virtual machine or across a cluster of nodes in high availability.

Livepatch Client will be unable to communicate with any Livepatch Server without Ubuntu Pro. With Ubuntu Pro, Livepatch Client can be enabled to download security patches from any Livepatch Server: on public cloud, Canonical's cloud, or on-premise.

THE VALUE PROPOSITION FOR LIVEPATCH

Safety-first architecture

Snap packages are confined and self-contained tamper-proof (read only) file system images that are GPG signed. Snap packages are very secure because they run in a sandboxed environment; system access is denied by default and the System Administrator controls what a Snap package is allowed to access, through pre-defined Snap interfaces.

Livepatch Client is packaged as a snap. As with all snap packages, it benefits from a built-in backup mechanism for its own application data, and has the ability to rollback automatically if the upgrades to the next Landscape Client version fails for any reason. Just like every other snap package, its self-updating capabilities can be controlled through Landscape, or a self-hosted Snap Store called the Enterprise Store. Such problems are rare, because Livepatch Client dependencies can never be broken: every dependency for Livepatch Client is also included in the snap package.

Incremental patching

Machines with patches selectively applied get comprehensively protected against all critical and high kernel vulnerabilities. The Livepatch Client identifies which patches are missing, and applies a Livepatch that is customized for that specific combination of installed security patches.

Canonical Livepatch packaging is never emulated

Every combination of Livepatch updates is tested natively on the target CPU architecture. Each build could take up to 50 minutes per release. Canonical's Kernel Engineering team packages Livepatch updates with the same rigor and process that goes into the Linux kernel itself: Livepatch updates are built with the same compiler as the kernel they are intended for. Canonical's Livepatch updates are stable and reliable, because they are never cross-compiled or created with architecture emulation.

COMMON USE CASES

Security patches for medium or below kernel vulnerabilities, glibc, CPU microcode, the grub bootloader, and other low-level system components all require a reboot to finalize the upgrade. However, high and critical kernel vulnerabilities can be addressed without a reboot with Canonical Livepatch.

Canonical Livepatch reduces the frequency of required reboots between security maintenance patching windows for the high and critical Linux kernel security patches, and dramatically reduces the exploit window of Linux kernel vulnerabilities.

SUPPORT AND COMPATIBILITY WINDOWS

Canonical's Kernel Team strives to support all use cases for the generic kernel. When the GA kernel is not suitable, kernel variants are created. For example: cloud-specific kernels benefit from improved mechanisms in performance or security that are material to that cloud. *Livepatch will work on any virtualized or bare-metal Ubuntu instance running on AMD64 or s390x CPUs, with GA or HWE kernels in public clouds and on-premises.*

The general availability (GA) kernel is the default kernel for Ubuntu Server, and ships with Ubuntu LTS upon its release, and remains at that major version for the life of that Ubuntu release. The hardware enablement (HWE) kernel is the default kernel for Ubuntu Desktop and virtual machines on Azure, Google, IBM, and Oracle public clouds. The HWE kernel is updated after 10 months with the 2nd point release of the Ubuntu LTS. A new HWE kernel is published with every subsequent Ubuntu LTS point release, every 6 months in August and February. The fifth point release is typically the last point release for Ubuntu LTS, and that version of the HWE kernel is slated to be the GA kernel for the next Ubuntu LTS release.

Kernel version	Type	Ubuntu release	Release Date	Max security coverage duration	Previous release
4.15	GA	18.04.0 LTS	Apr 2018	Apr 2030, upgrade and reboot every 13 months	
4.18	HWE	18.04.2 LTS	Feb 2019	Nov 2019, upgrade and reboot every 9 months	18.10
5.0	HWE	18.04.3 LTS	Aug 2019	May 2020, upgrade and reboot every 9 months	19.04
5.3	HWE	18.04.4 LTS	Feb 2020	Nov 2020, upgrade and reboot every 9 months	19.10
5.4	HWE	18.04.5 LTS	Aug 2020	Apr 2030, upgrade and reboot every 13 months	20.04.0 LTS
5.4	GA	20.04.0 LTS	Apr 2020	Apr 2032, upgrade and reboot every 13 months	
5.8	HWE	20.04.2 LTS	Feb 2021	Nov 2021, upgrade and reboot every 9 months	20.10
5.11	HWE	20.04.3 LTS	Aug 2021	Apr 2030, upgrade and reboot every 9 months	21.04
5.13	HWE	20.04.4 LTS	Feb 2022	Nov 2022, upgrade and reboot every 9 months	21.10
5.15	HWE	20.04.5 LTS	Aug 2022	Apr 2032, upgrade and reboot every 13 months	22.04.0 LTS
5.15	GA	22.04.0 LTS	Apr 2022	Apr 2034, upgrade and reboot every 13 months	
5.19	HWE	22.04.2 LTS	Feb 2023	Nov 2033, upgrade and reboot every 9 months	22.10
6.2	HWE	22.04.3 LTS	Aug 2023	May 2024, upgrade and reboot every 9 months	23.04
6.5	HWE	22.04.4 LTS	Feb 2024	Nov 2024, upgrade and reboot every 9 months	23.10
6.8	HWE	22.04.5 LTS	Sep 2024	Apr 2034, upgrade and reboot every 13 months	24.04.0 LTS

Ubuntu must be upgraded and rebooted within a 13-month rolling window when using a GA kernel, and must be upgraded and rebooted within a 9-month rolling window when using an HWE kernel.

Enabling Canonical Livepatch and scheduling security maintenance windows with a full upgrade and reboot every February and August aligns with the kernel release schedule, and ensures secure software is running.

GET STARTED

Livepatch is available for all Ubuntu instances with Ubuntu Pro, and can be enabled on demand:

```
$ pro enable livepatch
```

Canonical also offers professional consulting services to get you up and running with any type of Ubuntu deployment, as well as training to ensure your staff are ready to go live.

ADDITIONAL SERVICES

- Support offerings are available either on a 24/7/365 basis, or during business hours only.
- Landscape is provided as a multi-tenant service without an SLA, on Canonical's cloud.
- Landscape is provided as a service with an SLA as a Managed Application, either on-premises or in public clouds.

Find out more about Livepatch

Read Livepatch documentation

Watch the security patching best practices video on YouTube