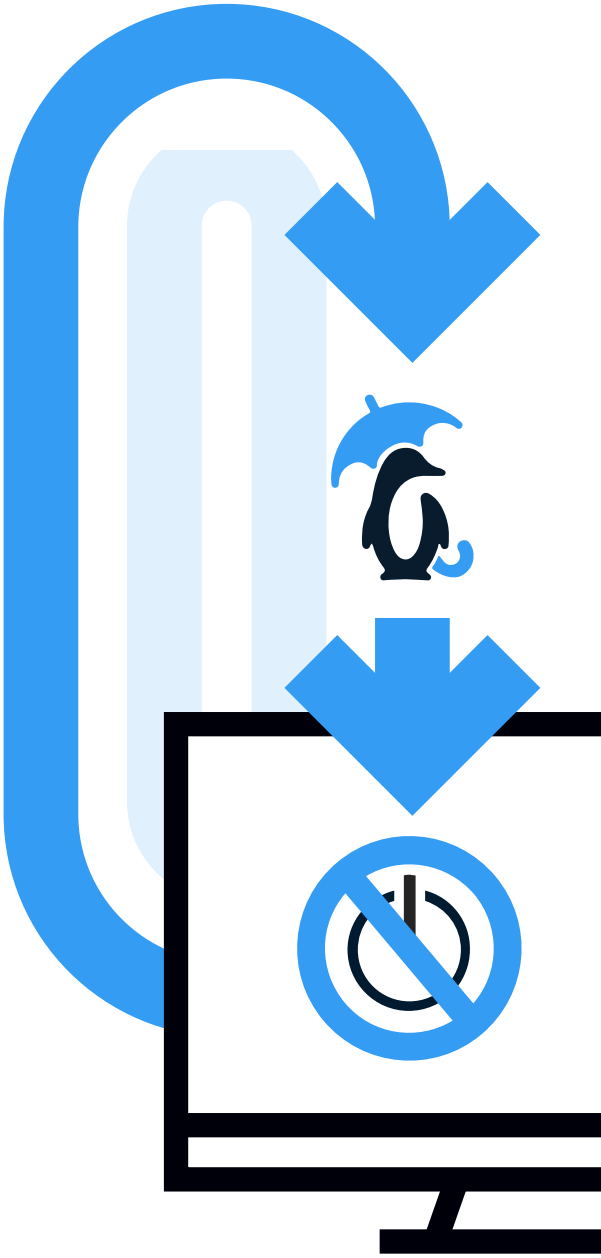
TuxCare
We Take Care of Linux

GUIDE

How Live Patching Works with KernelCare Enterprise

www.tuxcare.com

Introduction



TuxCare's live patching solution, KernelCare Enterprise, enables organizations to automatically apply vulnerability patches to many Linux-based systems while they're running, keeping them secure without needing to reboot them or schedule maintenance operations.

By automating these security updates and eliminating patching-related downtime, KernelCare Enterprise allows teams to apply patches as soon as they become available, spend less time and resources on routine patching processes, avoid end-user disruptions, and satisfy compliance requirements more easily.

KernelCare Enterprise delivers patches to all popular enterprise Linux distributions, including Red Hat Enterprise Linux, CentOS, Oracle Linux, AlmaLinux, Debian, Ubuntu, and many more. Plus, KernelCare Enterprise users can add live patching for IoT devices, databases, shared libraries like OpenSSL and glibc, and hypervisors in virtualized environments – like OpenStack.

But how does KernelCare Enterprise rapidly and reliably deliver vulnerability patches while these Linux systems are running?

In this document, you'll discover how TuxCare creates, distributes, and applies vulnerability patches automatically without reboots or downtime, as well as how to track our patch releases, get additional information on each patch, and more.

The KernelCare Enterprise Process

Our live patching solution delivers automated, non-disruptive patches to more than 40 Enterprise Linux distributions and thousands of kernels, with each patch consisting of all available security updates – old and new – so you never need to depend on tracking in kernel modules. In fact, KernelCare live patches can contain hundreds of individual patches.

But how does TuxCare build these patches before rapidly deploying them into your Linux hosts? Let's walk through the KernelCare patching process, step by step.

We Create the Patches

1

The TuxCare team identifies vulnerabilities by monitoring each Linux distribution vendor's kernel security fixes and dedicated security reporting channels.

2

We backport your kernel vendor's security fixes to ensure that your kernel stays as close as possible to your vendor's.

3

The code is compiled using the exact flags as the vendor's kernel and a 'live patch' is generated. In the simplest case, this patch may change one line of code, in others, e.g., Spectre and Meltdown mitigations, millions of lines of code are patched. Think of it as a binary diff generated between the official kernel version and the patched version.

4

A long testing process begins to ensure that the applied patches will not create any instability or break any workflows on the patched kernel.

5

After the quality assurance process is finished, the live patch is ready for release and becomes available for deployment in systems, either manually or automatically.

We Distribute the Patches

KernelCare Enterprise users receive their patches through two different channels, depending on their needs: either directly through portal.tuxcare.com or – for environments that aren't connected to the internet – via the TuxCare ePortal on-prem patch server.

Directly via portal.tuxcare.com

Customers register their system with a very simple command:

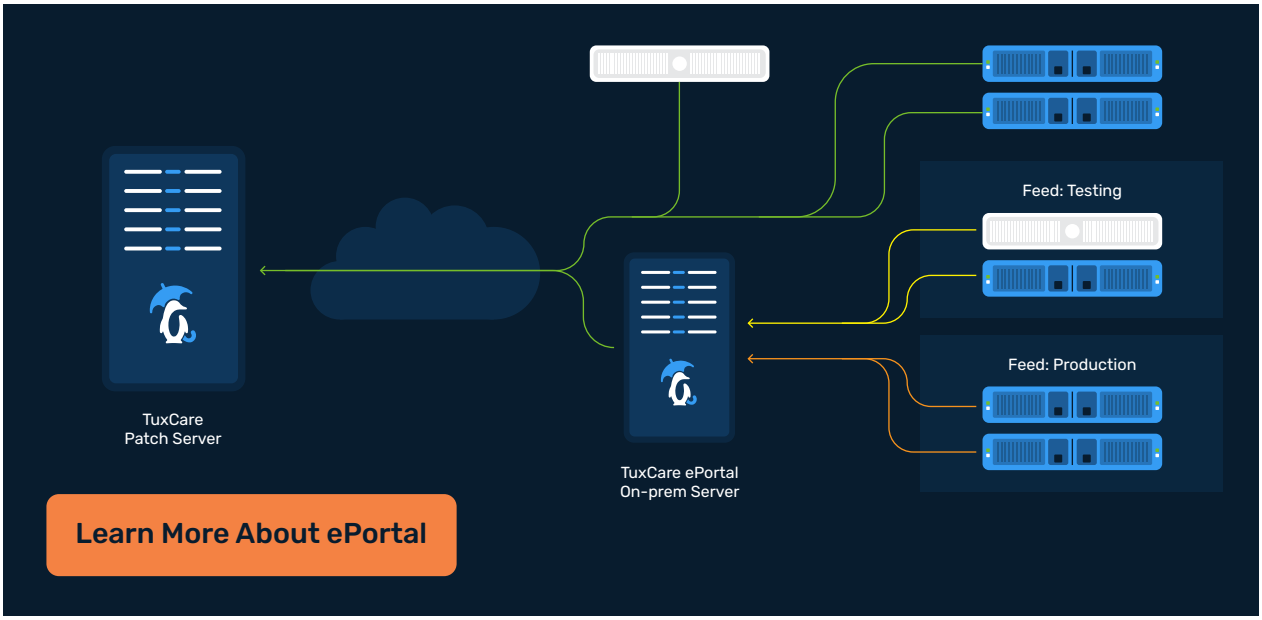
```
$ /usr/bin/kcarectl --register KEY
```

This ensures that their system starts receiving live patches immediately. There is no additional service running into a system – the system is configured to retrieve these live patches from the TuxCare patch server periodically via a cron job. There is also no permanently running "agent" taking up system resources. The task run from cron will run briefly and terminate until the next scheduled check.

Via ePortal

Because enterprise systems often have to follow specific patch deployment and roll-out policies or are in an air-gapped environment – or a restricted network – and unable to reach the general Internet, patches are deployed through the TuxCare ePortal.

ePortal is an on-prem server that handles the communication with the TuxCare patch server, assigning the systems into feeds, with each feed having its own deployment policy.



We Apply the Patches

Each Linux server with KernelCare Enterprise enabled has the `kmod_care` kernel module inserted, which executes the live patching process once the live patch is received on the Linux server. The live patch application process looks like this:

First

The module detects when the old vulnerable code is not in use. This ensures there is no consistency problem with having two different code blocks for the same function running simultaneously.

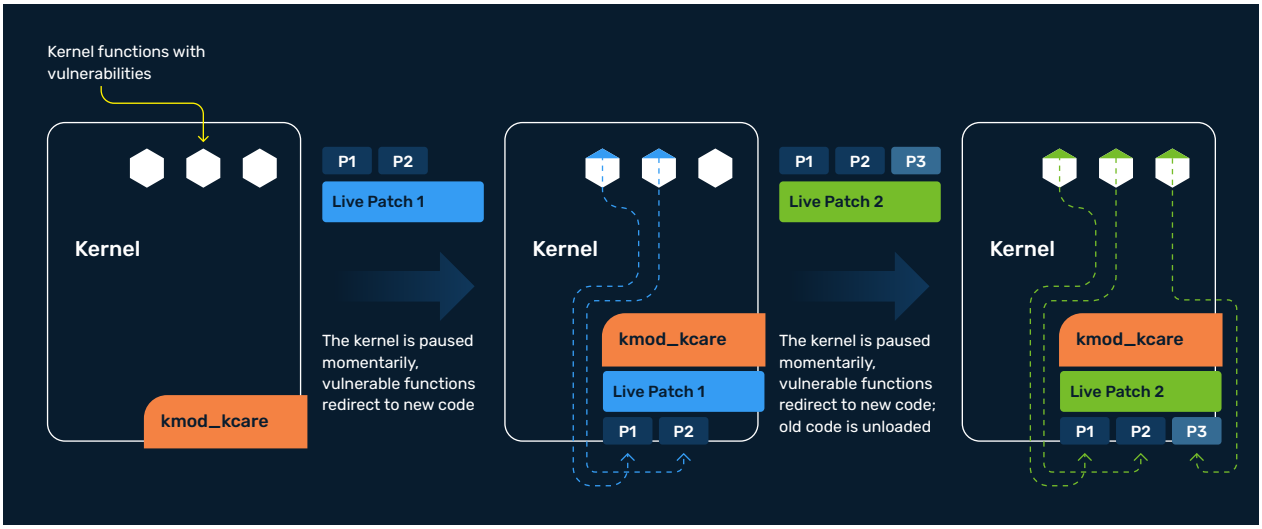
Second

The module pauses the kernel for mere microseconds and replaces the old code with the new non-vulnerable code. During the momentary pause, the vulnerable functions are modified to redirect to new code in the live patch.

And that's it!

Because this happens instantly, no processes are interrupted and no failover condition is ever triggered.

If you are familiar with the Linux upstream live patching techniques, our process follows a different consistency model; with `kmod_kcare` there is a point in time after which all the patches are applied to the entire system, whereas the upstream model has a gradual rollout of the new code.



Using KernelCare Enterprise Alongside Vulnerability Scanners

Organizations perform regular vulnerability scanning to evaluate their risk reduction efforts, which is why TuxCare has made sure KernelCare Enterprise live patches are visible to all major vulnerability scanners, including Qualys, Rapid7, and Tenable.

How do we get our live patching data to these platforms?

First, we provide data (in OVAL format) that instructs the vulnerability scanners on how to detect the presence of our vulnerability patches. Then, when the vulnerability is addressed by KernelCare, the scanning platforms get the right information – so the vulnerability reports our users download from their scanners don't falsely report a vulnerability that's already been patched by KernelCare Enterprise.

Learn More

KernelCare Enterprise Transparency

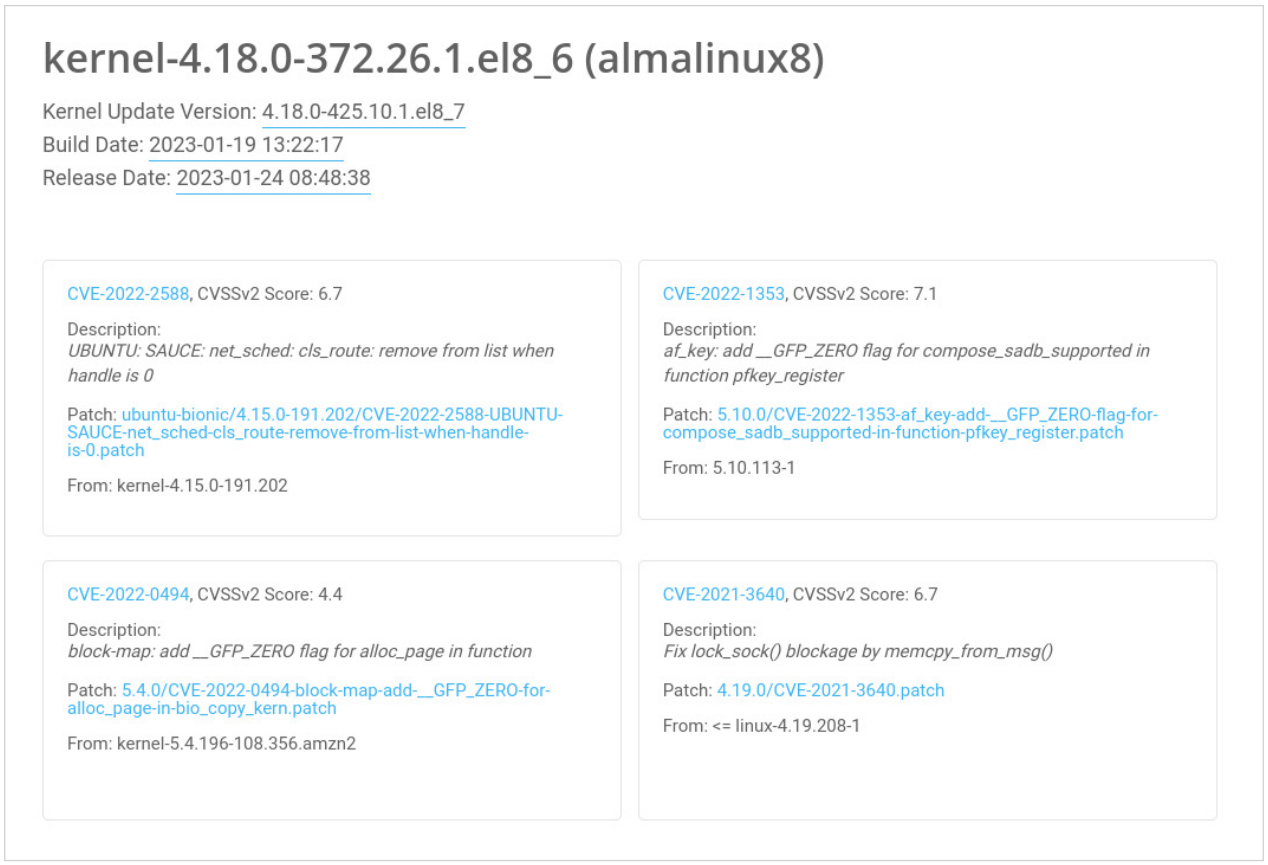
TuxCare is dedicated to providing full transparency when it comes to our patches and associated source code. To achieve this, we make sure that all details about each patch are available for KernelCare Enterprise users, including what is contained in each live patch, what vulnerabilities are addressed, and the source code of our software.

How Can I Find What Patches are Included in a Live Patch?

To find out all the patches and CVEs associated with any of our live patches, we provide a dedicated command: `kcarectl –patch-info`

Using this command will display all of the relevant information for the live patch applied into the current system.

Additionally, all live patches released by KernelCare Enterprise are available at patches.kernelcare.com. Clicking on the "Boot version" column shows the release date as well as a breakdown of the vulnerabilities the patch fixes and the associated patches.



Learn More

How Can I Find Which Vulnerabilities Are Addressed by KernelCare?

All the vulnerabilities addressed by KernelCare are available at cve.tuxcare.com/live

To make navigating this hub easier, you can filter by operating system, CVE, and kernel version.

Is KernelCare Enterprise Source Code Open Source?

Yes it is! We make the source code available not only for audit and review, but also under the open source GNU General Public license. The latest source code is available at:

- https://patches.kernelcare.com/libcare.tar.gz
- https://patches.kernelcare.com/kmod_kcare.tar.gz

Why TuxCare?

With TuxCare's family of enterprise Linux security solutions, organizations can automate vulnerability patching, minimize downtime, keep their applications secure and compliant, and get support from a team that knows Linux security best – covering their entire Linux estate, including most popular distributions, end-of-life systems, devices, libraries, and much more.

With the **KernelCare Enterprise** live patching solution, teams can put patching on autopilot for most popular distributions while avoiding downtime, disruptions, and unnecessary maintenance windows.

Extended Lifecycle Support (ELS) enables organizations to continue securely using Linux distributions and software languages that have reached end of life or no longer receive standard security support – delivering vulnerability patches for unsupported versions of CentOS, CentOS Stream, Ubuntu, Debian, Oracle Linux, PHP, and Python.

Our **Enterprise Support for AlmaLinux** offers the commercial support your business needs with break/fix support, automated live patching, extended security updates, continuous compliance, and pay-as-you-go hourly support bundles – giving you access to skilled AlmaLinux security experts whenever you need them.

With **SecureChain for Java**, companies gain access to a single trusted repository of independently verified and vulnerability-free Java packages and libraries, fully compliant with the NIST Secure Software Development Framework – so they can continue to innovate while maintaining the security of their applications.

LEARN MORE AT
www.tuxcare.com