Guide

TuxCare

How the Modern SysAdmin Does Patching

Reducing Work Hours and Minimizing Stress with Rebootless Patches

Discover how Linux System Administrators can significantly reduce their patching-related working hours and intelligently leverage automation with rebootless patching – a non-disruptive patching approach that puts vulnerability fixes on autopilot so that teams can spend more time on other critical tasks.

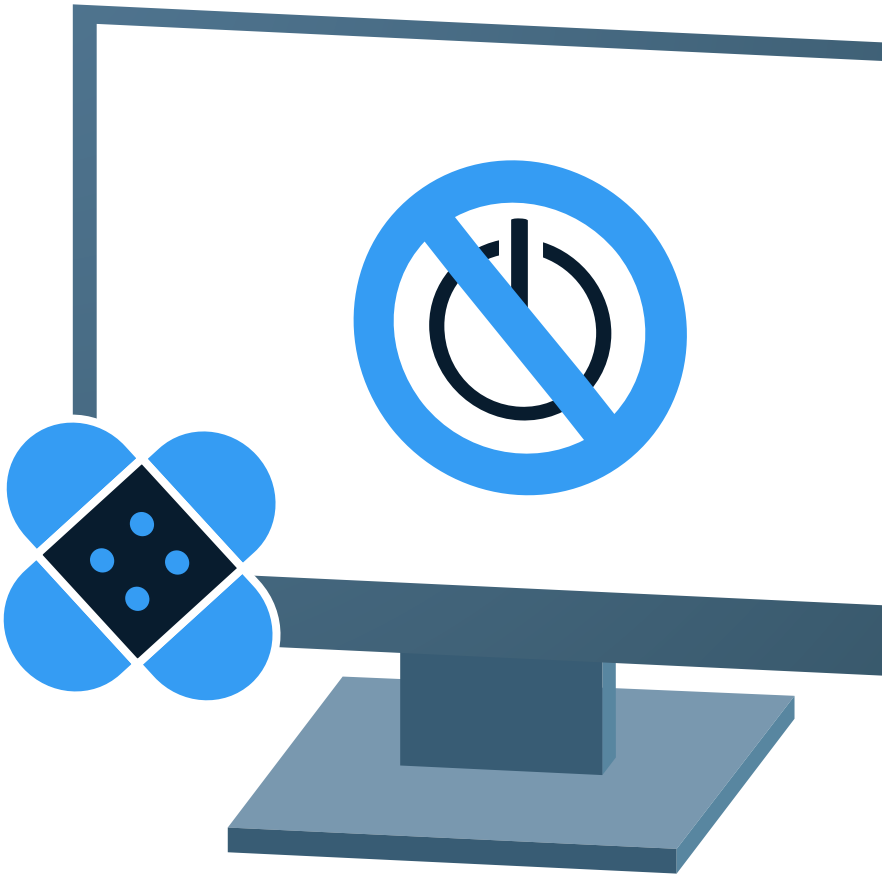

Table of Contents

Traditional Patching: A Never-Ending Headache for SysAdmins

For enterprise SysAdmins, managing Linux security patching has long been a demanding and ongoing challenge across organizations of all sizes. The pressure of the ever-present risk of sophisticated cyberattacks combined with the time-consuming nature of traditional patching methods makes it difficult to meet compliance deadlines and maintain security.

In conventional Linux kernel patching, SysAdmins must plan for system reboots – a process that often requires team members to babysit operations during off-hours or weekends. Coordinating these reboots across departments can become a logistical headache, and the difficulty of scheduling downtime before compliance deadlines means that non-compliance penalties are also a constant danger.

At the same time, delaying patches to align with reboot schedules often leaves systems vulnerable for longer than necessary, extending the window of risk for potential vulnerability exploits. This cumbersome process not only wastes valuable time but also increases the risk of potential exploitation during the window of vulnerability.

Fortunately, with rebootless patching, which is a modernized Linux vulnerability patching approach also referred to as "live patching," SysAdmins can focus on developing and deploying new technologies rather than babysitting existing ones – all while making it easier to demonstrate compliance and minimize the risk of vulnerability exploits.

What Is Rebootless Patching?

Faced with the downtime, disruptions, inefficiencies, and the risk of non-compliance that the conventional vulnerability patching approach introduces, SysAdmins at some of the world's most innovative enterprises have turned to rebootless patching as their solution.

Rebootless patching is an automated, non-disruptive patching approach that doesn't require reboots, downtime, or manual patching workflows. With a rebootless patching solution, all the latest patches can be automatically applied in the background, while systems are running, so that teams can "set it and forget it" while focusing their attention on other important tasks.

After SysAdmins adopt rebootless patching, there's no more babysitting reboots, interrupting important long-running operations, scheduling inconvenient maintenance windows across multiple departments, or wasting their teams' time on an outdated security approach.

The ability to deploy security patches without disruptions as soon as they are available not only reduces unnecessary patch delays and helps companies stay compliant with regulatory patching requirements, but also enables organizations to completely avoid reboots. Some companies that use KernelCare Enterprise rebootless patching, for example, have been able to keep their systems patched without rebooting for over nine years.

The Benefits of Rebootless Patching for SysAdmins

Avoid Burnout

By leaving behind the conventional patching approach, which isn't an efficient use of time or resources, your team can gain a more manageable workload.

Reduce Risk

Patching Linux kernel vulnerabilities quickly after patches are released allows your organization to minimize the window of opportunity for malicious entities to exploit them.

Patch Faster

Deploy security patches as soon as they're available, automatically – without disruptions or delays – so that you don't need to wait for a hard-to-coordinate maintenance operation.

Stay Compliant

By accelerating your patching timeline, you'll make it easier to comply with regulatory regimes that require companies to patch within a certain amount of time after a patch becomes available.

Minimize Downtime

By eliminating the need for system reboots, rebootless patching ensures near-constant system availability, which is crucial for businesses that require 24/7 uptime.

How Rebootless Patching Works

Rebootless patching with KernelCare Enterprise replaces code that contains vulnerabilities with new, secure code while your Linux kernel is running – eliminating the need for a system reboot.

The KernelCare Enterprise rebootless patching process looks like this:

1

We Create the Patch

We create code that patches insecure kernel code with a secure but functionally equivalent replacement.

2

We Prepare the Patch for Deployment

We compile every patch that impacts the affected kernel and deploy it to our distribution servers.

3

You Receive the Patch

A KernelCare process running on your server checks our distribution servers every 4 hours (by default). If a new patch is available, it can then be downloaded and applied to your running kernel – a process that can be automated.

4

KernelCare Applies the Patch

The patch is passed to the KCE kernel module, which – in a matter of nanoseconds – pauses all processes, loads the updated binary into the secure kernel space, redirects all functions to the updated code – and the kernel resumes. Because this happens in nanoseconds, no processes are interrupted, and no failover condition is ever triggered.

And that's it!

Did you know that KernelCare Enterprise rebootless patching is compatible with most popular Linux distributions, including Debian, Red Hat Enterprise Linux, CentOS, Ubuntu, AlmaLinux, Oracle Linux, and many more?

Rebootless Patching Beyond the Linux Kernel

In addition to patching the Linux kernel, rebootless patching can be applied to other critical areas of your organization's Linux estate.

Unlike most rebootless patching providers, KernelCare Enterprise can be extended to shared libraries, IoT environments, databases, and QEMU-based virtualization systems.

LibCare	Minimize downtime and automate vulnerability patching for OpenSSL and glibc without needing to reboot systems or schedule maintenance windows
IoT Connected Devices	Patch your Linux-based enterprise Internet of Things (IoT) ecosystem without needing to take connected devices out of production
QEMU-based Virtualization Systems	Stay patched without needing to shut down or migrate the virtualization layer or reboot the hypervisor

Is Rebootless Patching Right for Your Team?

While the benefits are clear, implementing rebootless patching depends on the specific needs of your organization and your team, specifically. Factors such as the criticality of continuous uptime, the scale of your operations, and regulatory requirements should all be considered. For organizations with 24/7 operations or those under stringent compliance regulations, rebootless patching can be a game-changer.

By integrating rebootless patching into your organization's software maintenance and cybersecurity strategy, you can significantly enhance system availability, security, and overall business continuity.

There are a few Linux rebootless patching solutions out there, with most focusing on just one specific distribution each. KernelCare Enterprise, on the other hand, delivers rebootless patches to most popular enterprise Linux distributions at a fraction of the cost of premium support services from vendors like Canonical, Red Hat, and Oracle – which may also only support one or a few Linux distributions.

If you already have a premium support subscription from a major Linux distribution vendor, rebootless patching with those costlier options may be a better option for your organization. If you want to spend less on non-disruptive rebootless patching or run a Linux estate with multiple distributions, KernelCare Enterprise is likely the best option.

To start a free trial of KernelCare Enterprise, head to www.tuxcare.com