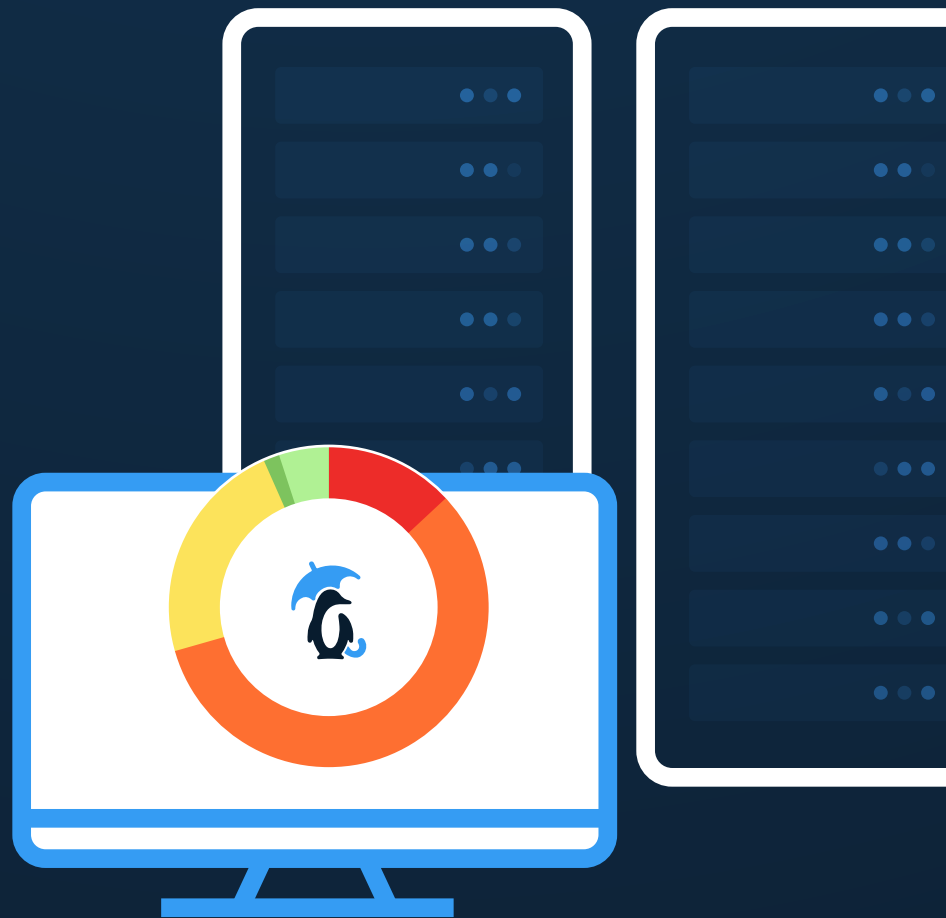




WHITEPAPER

Putting TuxCare Patching Solutions to the (Pen) Test



Summary

In cooperation with Governance, Risk, and Compliance (GRC) solutions provider C1Risk and Penetration-Testing-as-a-Service provider CYBRI, this experiment documents the significantly positive effect that TuxCare's vulnerability patching technologies have in reducing the composite risk scoring of a Linux OS host. To demonstrate this, multiple virtual machines (VMs) will undergo risk assessment before and after two different TuxCare patching solutions have been applied.

Each Linux OS used in this experiment will have several vulnerabilities, and the shift in risk scoring will be measured over a 30-day period. The scoring model comprises several factors captured within the C1Risk GRC tool.



The Problem with Patching

Enterprise Linux users know that vulnerability patching is essential to maintaining a secure and compliant organization. Patching is very effective in closing security gaps, but for a number of reasons many organizations find that they're unable to perform patching workflows as often as they should.

Limited resources and understaffing may be challenges that impede a company's ability to patch everything as soon as they can, but the act of planning and applying a Linux kernel patch can cause even more challenges – like end-user disruptions, deterioration of system performance, and even errors.

Plus, teams need to prioritize the vulnerabilities that they are going to patch first. With so many vulnerabilities appearing so frequently, it can be tricky to form an action plan on how to address them and in which order to do so. Combine this prioritization conundrum with the possible business impacts mentioned above, and you've got a recipe for delayed – or even completely neglected – vulnerability patches.

Fortunately, with the two TuxCare patching solutions that have been put to the test in this experiment, organizations can gain access to automatable, ready-to-deploy patches that eliminate much of the manual work involved in patching. Additionally, for many distributions, TuxCare's live patching technology enables patching with zero disruptions, zero downtime, and no need to prioritize which patches get deployed first.

So, which TuxCare patching solutions were used in this experiment and how did we evaluate them?

Testing Platforms Used in this Experiment

To execute this experiment, TuxCare launched four VMs running Enterprise Linux distributions within a virtualized environment. To apply vulnerability patches to these machines, one of two TuxCare solutions was installed:



KernelCare Enterprise


TuxCare’s flagship live patching solution, which applies vulnerability patches to the Linux kernel while it’s running in memory so that the host does not need to be rebooted to apply each patch.



Extended Lifecycle Support


TuxCare’s patching solution for end-of-life Linux distributions, which provides a repository of updated packages for Linux distributions that have reached the end of their vendor-provided support lifecycle and no longer receive patches from the original distribution vendor.

The following VMs deployed for this experiment were assigned one Linux distribution and one TuxCare patching solution based on how recent the distribution is, representing the vastly differentiated environments present in Enterprise IT infrastructure:




Ubuntu 16.04

Patching Solution:
TuxCare Extended Lifecycle Support




Ubuntu 20.04

Patching Solution:
TuxCare KernelCare Enterprise



CentOS 6.10

Patching Solution:
TuxCare Extended Lifecycle Support



CentOS 8.5

Patching Solution:
TuxCare KernelCare Enterprise



Understanding the Composite Risk Score

Within each of the targets, there is a composite risk score, which is generated both before and after TuxCare solutions have been installed. This score is generated by combining the risk score and the impact score.

The risk score factors in two attributes, including:

- Criticality of the host: high, medium, or low priority
- The aggregate of the CVE scores reported in the findings

The impact score considers the following attributes:

- Days opened
- Expected date of remediation: within 30 days, which was chosen as a metric as a currently accepted practice in the industry

Pre-TuxCare Composite Scores

A core component of this case study required extensive data collection and risk analysis to determine the initial composite score of each target. Before the TuxCare instance became activated, the cloud engineering team uploaded the specific details about each target VM into the C1Risk GRC tool. This is enabled manually or via API integration with C1Risk's platform.

C1Risk's platform executed its first pass at determining each machine's initial risk score (out of 100). The higher the score recorded, the greater the risk to the Linux OS.

Asset ID	Description	Composite Score	Asset Criticality	Assessment Date
ASR-001632	CentOS 8.5 (KC)	75	High	01/10/2023
ASR-001631	CentOS 6.10 (ELS)	75	High	01/10/2023
ASR-001630	Ubuntu 20.04 (KC)	85	High	01/10/2023
ASR-001629	Ubuntu 16.04 (ELS)	80	High	01/10/2023

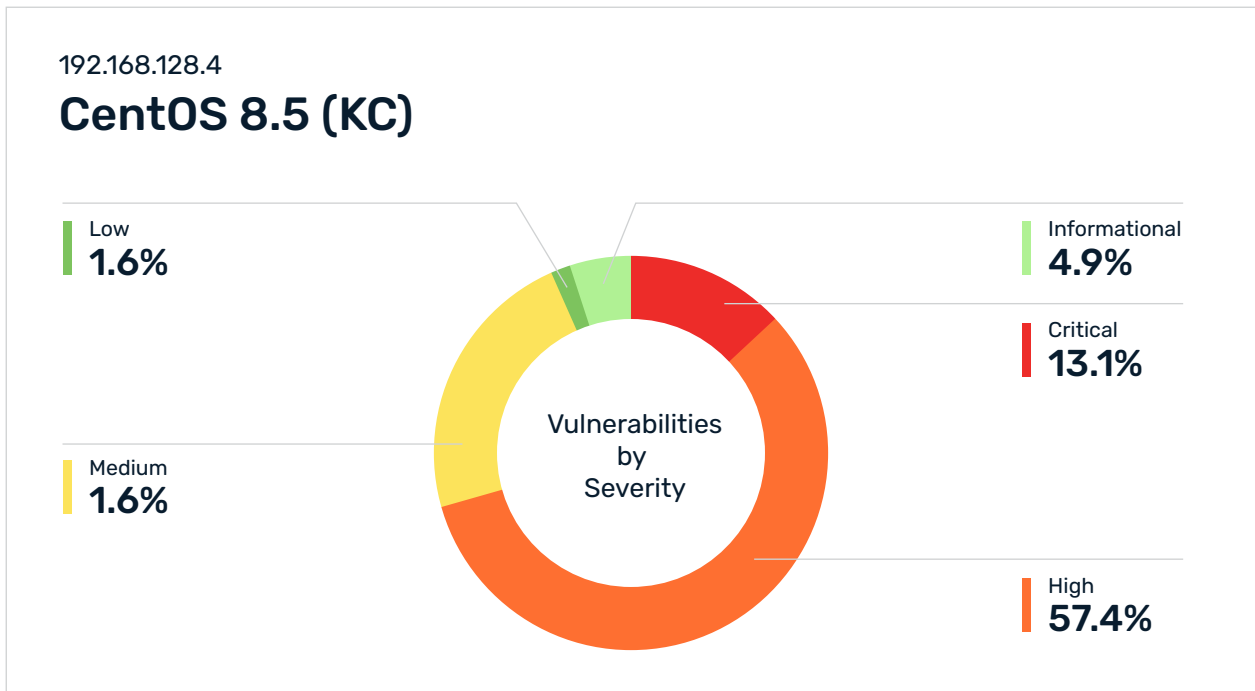
Once the GRC tool captured the asset and compiled the initial score, C1Risk collected the initial findings via API from CYBRI, an ethical hacking firm. Results were associated with risks, and action plans (mitigation and patching) were monitored in the platform.



C1Risk Engagement Synopsis

The findings reported within the C1Risk GRC platform resulted from several pen testing and vulnerability scanning events executed by CYBRI. C1Risk's platform ingested, via API, the findings from the pen testing and scanning, then provided TuxCare the ability to capture the initial composite risk score before the target test machines received patching from either KernelCare Enterprise or Extended Lifecycle Support. C1Risk tracked, monitored, and enabled risk scores to be updated based on patching and mitigation. The platform could monitor and show where risk automation was effective as well as where manual risk management was necessary.

Below is an example of the risk from one the four target hosts before TuxCare's patching solution was installed.



C1Risk's findings demonstrated the need for both manual and automated risk management. While they showed automation would work to decrease risk, some gaps required a manual approach, notably:



Non-supported packages for auto-patching



Out-of-scope software



CYBRI Engagement Synopsis

CYBRI's pen test method starts with discovering web application risks. CYBRI classified the found vulnerabilities according to The Ten Most Critical Web Application Security Risks from the Open Web Application Security Project (OWASP) Top 10 (2017), including vulnerable software and hardware components. Their white-hat engagement model uses a manual approach to discover and examine web application feature sets and technical security controls per the OWASP Application Security Verification Standard (ASVS) Project. All of CYBRI's pen testing team members work independently under the supervision of a team leader assigned to this experiment.

Remediation Stage Results

After installing TuxCare's two patching solutions, the following results were generated:

Name	TuxCare Remediation Strategy	Initial Composite Risk Score	% of Remediation	Remaining Composite Risk Score %
Critical (9.0-10 Base Score) CentOS 6.0	Extended Lifecycle Support (ELS)	85	100	0%
High (7.0-8.9 Base Score) for CentOS 6.10	Extended Lifecycle Support (ELS)	75	100	0%
Low (0.1-3.9 Base Score) for CentOS 6.10	Extended Lifecycle Support (ELS)	75	95	4%
Critical (9.0-10 Base Score) for Ubuntu 16.04	Extended Lifecycle Support (ELS)	80	100	0%
High (7.0-8.9 Base Score) for Ubuntu 16.04	Extended Lifecycle Support (ELS)	80	100	0%
Low (0.1-3.9 Base Score) for Ubuntu 16.04	Extended Lifecycle Support (ELS)	80	95	4%
Critical (9.0-10 Base Score) for CentOS 8.5	KernelCare Enterprise	75	100	0%
Medium (4.0-6.9 Base Score) for CentOS 8.5	KernelCare Enterprise	75	100	0%
Low (0.1-3.9 Base Score) for CentOS 8.5	KernelCare Enterprise	75	90	8%
Critical (9.0-10 Base Score) for Ubuntu 20.04	KernelCare Enterprise	85	100	0%
Medium (4.0-6.9 Base Score) for Ubuntu 20.04	KernelCare Enterprise	85	100	0%
Low (0.1-3.9 Base Score) for Ubuntu 20.04	KernelCare Enterprise	85	90	6%

As you can see, each target VM composite risk score was reduced significantly across the critical, high, and low categories. In all four VMs, for critical, high, and medium-level CVEs, the post-TuxCare composite risk score was 0%. For low-risk CVEs, the post-TuxCare composite risk score was incredibly low – between 4% and 8% across the four VMs.



Conclusion

By executing this experiment with four VMs and one of two TuxCare patching solutions, either KernelCare Enterprise or Extended Lifecycle Support, we have demonstrated that all critical, high, and medium-level vulnerabilities were completely eliminated from all machines involved.

For organizations that want to minimize their cybersecurity risk for both currently-supported Linux distributions and end-of-life distributions, TuxCare's patching solutions can drastically reduce your composite risk scores.

When it comes to distributions that have reached the end of their vendor-supported lifecycles, there would be no solution to existing security problems short of fixing the code, compiling it, and manually deploying the fixed applications directly. The benefit from having ready-to-deploy updated packages from TuxCare via Extended Lifecycle Support is obvious.

For currently in-support distributions, the benefit is not so much in the availability of a security fix, but rather in the possibility of deploying those fixes in a completely non-disruptive way through live patching.

TuxCare's live patching solution, KernelCare Enterprise, enables companies to deploy all the latest patches without needing to schedule downtime or execute a reboot – so your team can put patching on autopilot so that it runs in the background and no maintenance windows need to be coordinated. Additionally, KernelCare Enterprise provides live patching for all popular Enterprise Linux distributions in use today.

Moreover, this experiment demonstrates the value of having a Governance, Risk, and Compliance (GRC) platform like C1Risk and third-party penetration testing as a service provider like CYBRI assess the effectiveness of a cybersecurity solution. Organizations that provide security services must assess the strength of their technologies regularly to ensure that they are providing value to their customers.



About TuxCare

TuxCare is a global leader in open-source security, providing unmatched expertise in patching for your entire Linux estate. We deliver security patches to popular Linux distributions, end-of-life systems, programming languages, and more – offering a comprehensive security solution for all your infrastructure needs.

With over 80,000 patches – and counting – delivered to our users, TuxCare’s solutions reduce vulnerability exposure, minimize downtime, eliminate patching-related disruptions, secure your open-source supply chain, and maintain system stability and compliance.

TuxCare protects the world's largest enterprises, government agencies, service providers, universities, and research institutions, safeguarding over a million workloads (and growing). Our mission is to drive continuous innovation through open-source technologies while minimizing the risk of cyber threats and serving as a trusted technology partner for innovative organizations across the globe.



LEARN MORE AT
www.tuxcare.com

About C1Risk

C1Risk is the global market leader in Governance, Risk, and Compliance (GRC), providing comprehensive risk solutions for Enterprise, Operational, ESG, Legal, HR, IT, and Cybersecurity – with a mission to simplify organizations’ risk and compliance management so they can build and maintain the trust of their stakeholders.

[Learn More](#)

About CYBRI

CYBRI is a US-based cybersecurity company helping businesses detect and remediate mission-critical vulnerabilities before they get exploited by hackers. CYBRI provides state of the art Penetration-Testing-as-a-Service performed by the CYBRI Red Team (CRT) as well as virtual CISO (V CISO) programs to ensure that all businesses receive this needed level of protection.

[Learn More](#)

