KernelCare Eliminates Vulnerabilities in Linux Kernels Without the Need to Reboot Servers

*KernelCare rebootless and automated kernel update service has released multiple patches for the vulnerability reported yesterday. Supports many Linux distributions.*

LAS VEGAS (PRWEB) May 02, 2018 -- KernelCare, a product of CloudLinux, the leading shared hosting OS developer, announced that it now fixes recent Linux vulnerability, disclosed yesterday, for multiple Linux distributions without the need to reboot servers. KernelCare customers have those vulnerabilities patched without the reboots that are required by Linux system vendors.

On May 1st, a new vulnerability CVE-2018-1000199, which can lead to corruption and DoS, was disclosed for Linux kernel. The error reported has illustrated exploits for x86 kernels, but other kernels can be affected as well. According to Andy Lutomirski, who discovered the vulnerability, “the bug itself is spread all over the place in the kernel in generic and arch code.”

KernelCare keeps Linux servers secure with all the latest kernel patches, including one for the above vulnerability, automatically applied to the running kernel without downtime. It ensures servers are on and available and eliminates interruption to critical applications, databases, and business processes.

“Our dedicated team of kernel developers work around the clock to deliver patches that fix vulnerability issues without customers needing to reboot servers,” - said Igor Seletskiy, CloudLinux CEO. “We are the only vendor supporting live patching for many distributions that has rolled out patches to fix some of the most critical vulnerabilities, such as Meltdown, and we are very proud of the Kernel experts we have on our team”.

Companies like Dell, Endurance, and LiquidWeb have been protecting their kernels against security vulnerabilities, such as Meltdown and Spectre, without reboots. Their kernels have been patched without costly and inconvenient application downtime. KernelCare delivers virtually no performance impact during updates. Launched 4 years ago, it supports most popular Linux distributions including CentOS and RHEL, Xen4CentOS, OpenVZ & Virtuozzo, Debian, Ubuntu, and others.

At the Interop ITX 2018 tradeshow in Las Vegas, NV, KernelCare is showcasing its ability to fix kernel security vulnerabilities without the need to reboot servers in multiple Linux distributions. The solution ensures servers are on and available and eliminates interruption to critical applications, databases, and business processes.

To learn more, visit kernelcare.com or visit booth #1019 in the Business Hall of Interop 2018 event.

About KernelCare

KernelCare keeps Linux servers secure with all the latest kernel patches automatically applied to the running kernel without downtime. It ensures servers are on and available and eliminates interruption to critical applications, databases, and business processes. KernelCare, at Interop ITX 2018 booth #1019, will showcase its ability to fix kernel security vulnerabilities, such as Meltdown and Spectre, without the need to reboot servers in multiple Linux distributions.
KernelCare is a product of CloudLinux, the maker of #1 OS for shared hosting providers. More information about KernelCare can be found at kernelcare.com.
Contact Information
Inna Gordin
Cloud Linux Inc
http://cloudlinux.com
+1 9739518266

Online Web 2.0 Version
You can read the online version of this press release here.