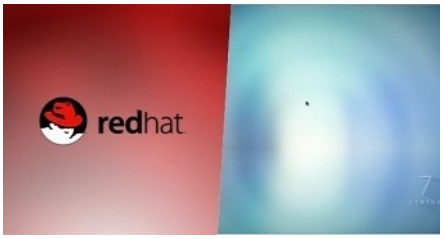
Red Hat Enterprise Linux 6 and CentOS 6 Receive Important Kernel Security Update

By *Rianne Schestowitz*
Created *18/09/2019 - 7:13pm*
Submitted by Rianne Schestowitz on Wednesday 18th of September 2019 07:13:41 PM Filed under Red Hat [1]



Marked by the Red Hat Product Security team as having a security impact of "Important," the new Linux kernel security update is here to patch a memory corruption (CVE-2018-9568) that occurred due to incorrect socket cloning and a NULL pointer dereference (CVE-2019-11810) discovered in drivers/scsi/megaraid/megaraid_sas_base.c, which could lead to a denial of service.

Also fixed in this update are two bugs affecting the performance of the Linux kernel on Red Hat Enterprise Linux 6 and CentOS Linux 6 systems, namely a fragmented packets timing out issue and the backport TCP follow-up for small buffers. These two bugs can be corrected if you install the new kernel versions for your operating system.

[2]

Red Hat

Links:
[1] http://www.tuxmachines.org/taxonomy/term/142
[2] https://news.softpedia.com/news/red-hat-enterprise-linux-6-and-centos-6-receive-important-kernel-security-update-527461.shtml