Red Hat Enterprise Linux 7 and CentOS 7 Receive Important Kernel Security Update

By *Rianne Schestowitz*
Created *27/02/2020 - 4:42am*
Submitted by Rianne Schestowitz on Thursday 27th of February 2020 04:42:57 AM Filed under Red Hat [1] Security [2]

The new kernel security update is marked as ?Important? by the Red Hat Product Security team and patches two heap overflows (CVE-2019-14816 and CVE-2019-14901) in the Marvell Wi-Fi chip driver.

While CVE-2019-14816 could allow an attacker on the same Wi-Fi physical network segment to cause a denial of service (system crash) or even maybe execute arbitrary code, CVE-2019-14901is more dangerous as it lets a remote attacker crash the system or execute arbitrary code.

[3]

Red Hat Security

Source URL: http://www.tuxmachines.org/node/134536

Links:
[1] http://www.tuxmachines.org/taxonomy/term/142
[2] http://www.tuxmachines.org/taxonomy/term/59
[3] https://9to5linux.com/red-hat-enterprise-linux-centos-kernel-security-update