Critical Linux Kernel Vulnerability Patched in Ubuntu 19.10 and 18.04.4 LTS

Discovered by Manfred Paul, the security vulnerability (CVE-2020-8835) was found in Linux kernel’s BPF (Berkeley Packet Filter) verifier, which incorrectly calculated register bounds for certain operations.

This could allow a local attacker to either expose sensitive information (kernel memory) or gain administrative privileges and run programs as root user.

The security issue affects all Ubuntu 19.10 (Eoan Ermine) and Ubuntu 18.04.4 LTS (Bionic Beaver) releases running Linux kernel 5.3 on 64-bit, Raspberry Pi, KVM, as well as cloud environments like AWS, Azure, GCP, GKE, and Oracle Cloud.
Links: