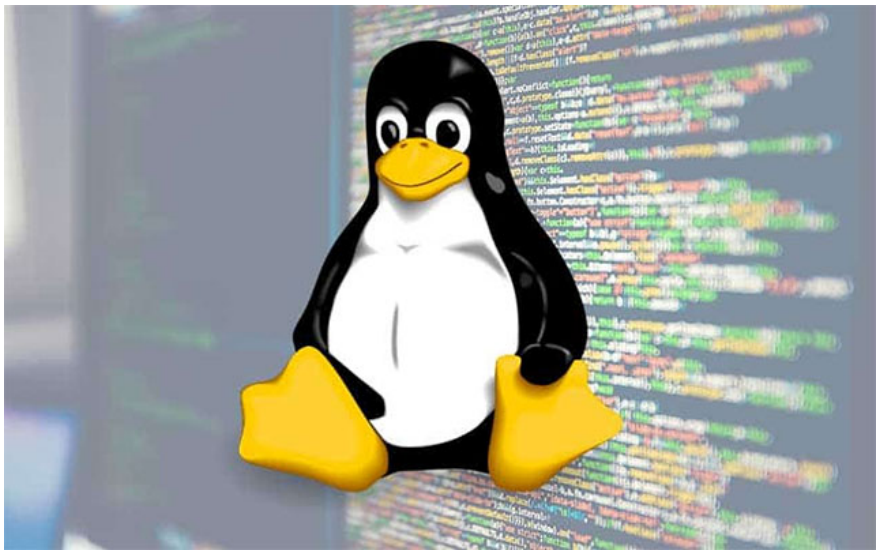
# Linux kernel vulnerability exposes Stack memory, causing local data leak

The way the researcher tells an international has just disclosed information about a relatively serious vulnerability that exists in the Linux kernel, which can be exploited to leak data and act as a bridge. Effective coupling for deeper penetration into victim systems.

First announced by researchers from cybersecurity organization Cisco Talos on April 27, this is essentially a disclosure vulnerability "that could allow attackers to gain access. Kernel's stack memory - a crucial component of Linux 'open source operating systems.



If you do not know, the stack memory acts as a storage place for local variables in functions, passed parameters . The process of accessing this memory is very fast, and is executed when the program translate. The size of the stack memory is fixed, depending on the particular operating system. For example, the usual stack memory of Windows is 1MB, while that of Linux is 8MB.

The vulnerability is currently being tracked with identifier CVE-2020-28588, and originated from the proc / pid / syscall function of 32-bit ARM devices running the Linux operating system in general.

According to the results of preliminary investigations by Cisco Talos experts, the first issue related to this vulnerability was discovered on a device running on Azure Sphere. Attackers who have sought to exploit the security vulnerability could read the file / syscall OS through Proc, a system used to communicate between nuclear data structures.

The / syscall procfs item can be abused if an attacker launches a command to output 24 bytes in the uninitialized stack memory, resulting in Kernel Address Space Layout Randomization (KASLR) bypassing.

The attack was "undetectable on the remote network" because it was essentially a legitimate Linux OS file being read, the researchers said.

"If used properly, an attacker can take advantage of this information leak to successfully exploit additional unpatched Linux vulnerabilities," the Cisco team added.

Linux kernel versions 5.10-rc4, 5.4.66, and 5.9.8 are directly affected by this vulnerability. Currently, a patch has been released to minimize the risks associated with the vulnerability. It is recommended that users update their builds to the latest version to ensure safety.