secpod

TOP LINUX KERNEL VULNERABILITIES - 2021

www.secpod.com

SECPOD CYBERHYGIENE REPORT

A story of vulnerabilities, patches, savage hackers, and undefeated sysadmins.

Linux Kernel is one of the crucial pillars of the open-source ecosystem and is used by IT communities across the globe. Unlike Windows and macOS, where updates are published automatically by the vendor, the case of Linux Kernels is different. Linux Developers in the IT communities look for these vulnerabilities, develop a fix, and share it with other members to deploy on their products. With the support of large open-source communities like this and a strict privilege system embedded in the architecture, Linux has always been considered a secure operating system.

However, with the constant changes in the IT demographics and changing security landscape, gone are those days when basic security practices were enough to safeguard a Linux environment. Over the years, the Linux operating system has caught the attackers' massive attention due to its rising popularity. A range of new Linux malware variants and attacks have emerged in recent years, keeping the Linux threat surface wide. Although the key reasons for these attacks can be attributed to misconfigurations and manual errors, Linux Kernel Security cannot be left unblamed.

Linux Kernel forms the foundation of the Linux Operating System, a core interface between computer hardware and its processes. Critical vulnerabilities in Linux Kernel will easily lead to privilege escalation and remote attacks. Continuous detection and remediation of these kernel vulnerabilities will safeguard the Linux ecosystem, preventing malicious security breaches.

WHAT THIS REPORT CONSISTS OF?

To help you strengthen your Linux security posture, we have put together a report on the Top Linux Kernel Vulnerabilities of 2021. The reports consist of the vulnerability CVE details, CVSS number, the affected products, and the impact of the vulnerability. Ensure that you immediately discover and remediate these vulnerabilities in your Linux network to prevent potential attacks.

TOP LINUX KERNEL VULNERABILITIES OF 2021

S.No	CVE ID	CVSS Score	Affected Product(s)	Impact
1	CVE-2021-33909	7.8	Ubuntu 20.04, Ubuntu 20.10, Ubuntu 21.04,Debian 11, RHEL 6, RHEL 7, RHEL 8 and Fedora 34 Workstation	A successful attack results in privilege escalation.
2	CVE-2021-43267	9.8	Linux, Fedora, NetApp products	Allows remote attackers to exploit insufficient validation of user-supplied sizes for the MSG_CRYPTO message type.
3	CVE-2021-33910	5.5	Systemd, Fedora, Debian, RHEL 8	This attack causes systems and the services it manages to crash and stop responding.
4	CVE-2021-45469	7.8	Debian Linux, Fedora, NetApp HCI Baseboard Management Controller (BMC) - H300S/H500S/H700S/H300E/H500E/H700E/H410S, NetApp HCI Baseboard Management Controller (BMC) - H410C	This can allow attackers to read sensitive information from other memory locations and cause a crash

S.No	CVE ID	CVSS Score	Affected Product(s)	Impact
5	CVE-2021-44733	7	Debian Linux, Fedora,NetApp HCI Baseboard Management Controller (BMC) - H300S/H500S/ H700S/H300E/H500E/H700E/H410S, NetApp HCI Baseboard Management Controller (BMC) - H410C	A local user could use this flaw to crash the system or escalate their privileges on the system
6	CVE-2021-3653	8.8	RHEL	Due to improper validation of the "int_ctl" field, this issue could allow a malicious L1 to enable AVIC support (Advanced Virtual Interrupt Controller) for the L2 guest. As a result, the L2 guest would be allowed to read/write physical pages of the host, resulting i n a crash of the entire system, leak of sensitive data or potential guest-to-host escape.
7	CVE-2021-39633	5.5	Android	This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.
8	CVE-2021-45485	7.5	Linux	Information leak
9	CVE-2021-39634	7.8	Android	This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation
10	CVE-2021-46283	5.5	Linux	A local user can set a netfilter table expression in their own namespace.

*Patches are available to remediate the Top Linux Kernel Vulnerabilities mentioned in the table.

DISCOVER AND REMEDIATE LINUX KERNEL VULNERABILITIES USING SANERNOW

It is essential to secure your Linux network before a wild security storm could attack via these vulnerabilities. SecPod SanerNow's continuous and automated vulnerability management solution enables you to detect the Linux vulnerabilities and remediate them on time using its integrated patch management. Leveraging the industry's fastest scans and homegrown world's largest vulnerability database, SanerNow swiftly manages the Linux threat surface keeping the attacks at bay. Along with Linux, SanerNow also supports other operating systems including Windows and macOS.

SCHEDULE A DEMO

Email us on: **info@secpod.com**, Call us at: India - **(+91) 80 4121 4020** / USA - **(+1) 918 625 3023**