Source : www.thehindu.com Date : 2022-08-24

CERT-IN ISSUES THREAT ALERT FOR HIGH SEVERITY VULNERABILITIES IN LINUX, UNIX AND REALTEK SDK

Relevant for: Science & Technology | Topic: Computer Technology incl. 3-D Printing

CERT-In issues threat alert for high severity vulnerabilities in Linux, Unix and Realtek SDK | Photo Credit: AP

Vulnerabilities in Linux and Unix can be exploited to execute arbitrary code while the critical vulnerability in Realtek could be affecting networking devices, revealed the Indian Computer Emergency Response Team (CERT-In) on Monday.

(Sign up to our Technology newsletter, Today's Cache, for insights on emerging themes at the intersection of technology, business and policy. Click here to subscribe for free.)

CERT-In released vulnerability notes for Linux, an open source operating system, Unix, a modular OS, and Realtek SDK, a software development kit.

The path traversal vulnerability in Linux and Unix reportedly exists in the RarLab's UnRAR utility tool. It can be exploited by attackers to execute arbitrary codes on the targeted systems.

Execution of arbitrary codes could allow attackers to gain access to sensitive information on the targeted system, compromising their security.

CERT-In noted that the vulnerability exists due to improper limitations in a pathname to a restricted directory.

RarLab, better known for developing WinRAR, shared on its website that the vulnerability does not affect WinRAR or Android RAR. It also released updates to fix the issue.

Hackers can exploit the vulnerability by sending crafted RAR files to a Zimbra server, thereby compromising their security, noted CERT-In's release.

A critical vulnerability has been reported in Realtek's Software Development Kit (SDK).

Attackers could misuse the vulnerability to generate a buffer or a stack overflow on an affected device. This could allow attackers to fill memory space that is otherwise kept out of bounds when a program transfers memory from one place to another.

CERT-In noted that the vulnerability exists due to improper bounds checking by the SIP ALG function. This in turn could allow an attacker to gain access and execute their own code on the targeted system.

The zero-click vulnerability can be exploited by sending specially crafted SIP packets containing SDP, a format for sending multimedia communication sessions through a broad area network

Application of relevant updates, acknowledged by Realtek, was recommended to fix the vulnerability.

END