مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Critical RCE Vulnerability in OpenSSH Linux systems

Tracking #:432316004

Date:02-07-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical remote code execution vulnerability has been identified in OpenSSH that could result in unauthenticated remote code execution with root privileges in glibc-based Linux systems.

TECHNICAL DETAILS:

A Remote Unauthenticated Code Execution (RCE) vulnerability **CVE-2024-6387** exists in OpenSSH's server (sshd) in glibc-based Linux systems, which is a signal handler race condition in OpenSSH's server (sshd), allows unauthenticated remote code execution (RCE) as root on glibc-based Linux systems; that presents a significant security risk. This race condition affects sshd in its default configuration.

Impact: Unauthenticated Remote Code Execution (RCE) with root privileges. This means an attacker can potentially take complete control of the affected system.
Affected Systems: OpenSSH server (sshd) on glibc-based Linux systems.

- Versions earlier than 4.4p1 (released 2006) unless patched for CVE-2006-5051 and CVE-2008-4109.
- Versions 8.5p1 (released March 2021) up to, but not including, 9.8p1 (released July 1st, 2024).

Fixed Version:

- OpenSSH 9.8/9.8p1

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade to fixed version at the earliest.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.openssh.com/txt/release-9.8