مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in NixOS Package Manager

Tracking #:432316288

Date:16-09-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in NixOS Package Manager that could be exploited to execute malicious code on affected systems.

TECHNICAL DETAILS:

A critical vulnerability exists in Nix, a popular package manager for Linux and Unix-based systems. This flaw allows attackers to write arbitrary files with root permissions, posing a significant risk to system security.

Vulnerability Details:

- **CVE-2024-45593**
- **CVSS Score:** 9.0 Critical
- The vulnerability resides in the NAR (Nix ARchive) unpacking process. Malicious users can craft specially designed NAR files that, when unpacked by Nix, can overwrite or create files anywhere on the system to which the Nix process has access. This becomes particularly dangerous when Nix is running as root, as in the case of using the Nix daemon.
- Successful exploitation of this vulnerability could allow attackers to gain elevated privileges, execute arbitrary code, and corrupt critical system files, potentially leading to data loss, system instability, or complete system compromise.

Affected Versions:

- Nix versions 2.24.0 through 2.24.5

Fixed Versions:

- Nix 2.24.6 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the affected versions to the fixed versions 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://nvd.nist.gov/vuln/detail/CVE-2024-45593