مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

High-Severity Vulnerability in TrueNAS CORE

Tracking #:432316692

Date:31-12-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in TrueNAS CORE, the widely-used open-source network-attached storage (NAS) operating system. This flaw could allow attackers to execute malicious code on affected devices.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-11944**
- **CVSS Score**: 7.5 (High)
- **Affected Component**: tarfile.extractall method
- **Vulnerability Type**: Directory Traversal / Remote Code Execution
- A security vulnerability exists in iXsystems TrueNAS CORE. This security flaw allows unauthenticated, network-adjacent attackers to remotely execute code on vulnerable TrueNAS devices.
- The vulnerability stems from inadequate validation of user-supplied paths in the tarfile.extractall method used for file operations. Attackers can exploit this flaw to craft malicious archives that, when processed, allow file system traversal and arbitrary file writing
- Successful exploitation can lead to:
    - Arbitrary code execution with root-level privileges
    - Unauthorized access to sensitive data
    - Installation of malware or backdoors
    - Corruption or deletion of critical system files

Affected Versions

- TrueNAS CORE versions prior to 13.0-U6.3

Fixed Versions:

- TrueNAS CORE installations to version 13.0-U6.3 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-2024-11944