مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in FreeBSD

Tracking #:432316317

Date:24-09-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed The FreeBSD Project has issued a security advisory to address a critical vulnerability affecting multiple versions of its operating system.

TECHNICAL DETAILS:

The FreeBSD Project has issued a security advisory to address a critical vulnerability (CVE-2024-4172) affecting multiple versions of its operating system.

Vulnerability Details:

- **CVE ID- CVE-2024-4172**
- **CVSS Score-9.8 (Critical)**
- An insufficient boundary validation in the USB code could lead to an out-of-bounds read on the heap, which could potentially lead to an arbitrary write and remote code execution.
- A malicious, privileged software running in a guest VM can exploit the vulnerability to crash the hypervisor process or potentially achieve code execution on the host in the bhyve userspace process, which typically runs asroot.

- **Affected Versions**: All supported versions of FreeBSD.

- **Fixed Versions:**
  - stable/14, 14.1-STABLE)
  - releng/14.1, 14.1-RELEASE-p5)
  - eleng/14.0, 14.0-RELEASE-p11)
  - stable/13, 13.4-STABLE)
  - releng/13.4, 13.4-RELEASE-p1)
  - releng/13.3, 13.3-RELEASE-p7)

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to update the affected products to the 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.freebsd.org/security/advisories/FreeBSD-SA-24:15.bhyve.asc