مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Code Execution Vulnerability in R Programming Language

Tracking #:432315811

Date:02-05-2024

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high severity vulnerability in the R programming language that could allow attackers to execute malicious code on a victim's system.

TECHNICAL DETAILS:

Vulnerabilities Details:

- **CVE-2024-27322 (CVSS 8.8.)-** Deserialization of untrusted data can occur in the R statistical programming language, on any version starting at 1.4.0 up to and not including 4.4.0, enabling a maliciously crafted RDS (R Data Serialization) formatted file or R package to run arbitrary code on an end user's system when interacted with.
- An attacker can create malicious .rds and .rdx files and use social engineering to distribute those files to execute arbitrary code on the victim's device.

Affected Products:

- R versions 1.4.0 up to, but not including, 4.4.0.

Fixed Versions:

- R version 4.4.0.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends update to the latest version of R as soon as possible.

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-2024-27322