مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Critical vulnerability in Curl Exposes User Credentials

Tracking #:432316647

Date:18-12-2024

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

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in the widely used curl command-line tool and library. This vulnerability could potentially expose user credentials under specific circumstances.

TECHNICAL DETAILS:

Vulnerability Details

- **CVE-2024-11053**
- CVSS Score: 9.1 (Critical)
- A critical vulnerability exists in curl that could lead to the exposure of user credentials when using .netrc files and following HTTP redirects.
- The issue occurs when curl is configured to use a .netrc file for credentials and follow redirects. Under specific circumstances, curl may leak the password intended for the initial host to the redirected host. This happens if the .netrc file has an entry for the redirect target hostname but omits the password or both the login and password.
- **Example scenario:**
    1. A curl transfer to a.tld redirects to b.tld
    2. The .netrc file contains:
       ```
       machine a.tld
       login alice
       password alicespassword
       default
       login bob
       ```
    3. In this case, curl would incorrectly use "alicespassword" for the transfer to b.tld

Successful exploitation of this vulnerability could lead to:

- **Unauthorized Access**: Malicious actors could gain access to sensitive systems and data.
- **Data Breaches**: Confidential information could be compromised.
- **Account Hijacking**: Accounts could be taken over by unauthorized individuals.

Affected Versions:

- curl versions 6.5 to 8.11.0

Mitigations:

- Upgrade curl and libcurl to version 8.11.1 or higher
- If upgrading is not possible, apply the provided patch and rebuild curl
- As a temporary workaround, avoid using .netrc files together with redirects

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-2024-11053