مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Heap buffer overflow Vulnerability in Perl

Tracking #:432317072

Date:14-04-2025

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 heap buffer overflow vulnerability (CVE-2024-56406) has been identified in multiple versions of the Perl programming language.

TECHNICAL DETAILS:

A heap buffer overflow vulnerability (CVE-2024-56406) has been identified in multiple versions of the Perl programming language. This flaw stems from improper handling of non-ASCII characters in the tr/// transliteration operator, which can be exploited to cause a segmentation fault, leading to Denial of Service (DoS). In less protected environments, this vulnerability may be leveraged for arbitrary code execution.

Vulnerability Details

- **CVE ID:** CVE-2024-56406
- **Severity:** High (CVSS Score Pending)
- **Affected Versions:** Perl 5.34, 5.36, 5.38, 5.40
- **Patched Versions:** Perl 5.38.4, 5.40.2
- **Vulnerability Type:** Heap Buffer Overflow
- **Vector:** Local execution with malformed input

Impact:

- Denial of Service: Crafted input triggers segmentation faults, crashing applications or systems.
- Code Execution: Potential exploitation in environments with weak memory protections (e.g., legacy systems).

RECOMMENDATIONS:

- Upgrade Perl to fixed or latest Version.

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-2024-56406