مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Remote Code Execution Vulnerability in Tinyproxy

Tracking #:432315831

Date:08-05-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability has been identified in Tinyproxy allows attackers to remotely execute code on vulnerable systems.

TECHNICAL DETAILS:

A critical vulnerability (CVE-2023-49606) has been identified in Tinyproxy versions 1.10.0 and 1.11.1. This flaw allows attackers to remotely execute code on vulnerable systems with unauthenticated requests. Over 50,000 vulnerable hosts are exposed on the internet, making this a significant security risk.

Details:

- **Vulnerability: CVE-2023-49606** (CVSS: 9.8) - Remote Code Execution (RCE)
- **Affected Software:** Tinyproxy versions 1.10.0 and 1.11.1
- **Exploitation:** Unauthenticated attackers can exploit this vulnerability with a specially crafted HTTP header to trigger memory corruption and potentially execute arbitrary code.
- **Impact:** Successful exploitation could allow attackers to take complete control of the affected system.

RECOMMENDATIONS:

- Update Immediately: Patch Tinyproxy to the latest version as soon as it becomes available.
- Disable Public Access: If Tinyproxy is not required to be accessible from the public internet, restrict access to internal networks only.
- Monitor Systems: Implement security measures to detect and prevent unauthorized access attempts.

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-2023-49606