مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Fluent Bit Memory Corruption Vulnerability ("Linguistic Lumberjack")

Tracking #:432315877

Date:22-05-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical security vulnerability nicknamed "Linguistic Lumberjack," exists in Fluent Bit, a popular logging and metrics collection tool. This vulnerability could allow attackers to crash the service, steal sensitive information, or potentially even execute malicious code on the affected systems.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-4323**
- **CVSSv3 Base Score 9.8 Critical**
- A memory corruption vulnerability exits in Fluent Bit's built-in HTTP server that can be exploited by a remote attacker to potentially crash the service (denial-of-service), leak sensitive information, or even execute arbitrary code on the system.
- The vulnerability resides in the built-in HTTP server of Fluent Bit and is exploitable by sending specially crafted requests to specific API endpoints, such as /api/v1/traces and /api/v1/trace. These endpoints handle trace data, and due to improper validation, an attacker can inject non-string values, leading to memory corruption.

Affected Versions:

- Fluent Bit versions 2.0.7 through 3.0.3

Fixed Versions:

- Fluent Bit version 3.0.4 or later.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the latest fixed version released by Fluent Bit.

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.tenable.com/security/research/tra-2024-17
- https://www.tenable.com/blog/linguistic-lumberjack-attacking-cloud-services-via-logging-endpoints-fluent-bit-cve-2024-4323