مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Critical Vulnerability in Xlight SFTP Server

Tracking #:432316451

Date:29-10-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability has been identified in the Xlight SFTP server, that can be exploited by unauthenticated attackers to gain code execution or cause a denial of service.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-46483**
- CVSS score of 9.8 Critical
- The vulnerability arises from how the Xlight SFTP server handles string lengths during the SSH handshake process. Specifically:
  - Strings sent over the SFTP protocol are prefixed with a four-byte length.
  - The function responsible for reading these strings encounters an integer overflow when validating the length and allocating the required memory.
- By crafting a malicious four-byte length for a string, an attacker can trigger a significant memory operation (approximately 4GB) that writes out-of-bounds onto the heap. This vulnerability is particularly concerning during pre-authentication phases when the server receives client data such as supported algorithms, cipher suites, usernames, and passwords.
- Exploitation of this vulnerability can allow an unauthenticated attacker to:
  - Gain code execution on the affected server.
  - Cause a denial of service, leading to system instability and crashes.
- A proof-of-concept exploit is publicly available on Github, making it easier for malicious actors to exploit this flaw.

Affected Versions:

- Xlight SFTP Server: All 32-bit and 64-bit versions <= 3.9.4.2

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to update Xlight FTP Server to the latest version immediately.

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://github.com/kn32/cve-2024-46483/blob/master/README.md