مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Authentication Bypass Flaw in ProjectSend

Tracking #:432316576

Date:28-11-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical authentication bypass vulnerability in ProjectSend, an open-source file-sharing web application, is being actively exploited by threat actors.

TECHNICAL DETAILS:

A critical authentication bypass vulnerability (CVE-2024-11680) in ProjectSend, an open-source file-sharing web application, is being actively exploited by threat actors. Despite being patched in May 2023, the vulnerability was only recently assigned a CVE, leaving many users unaware of its severity. Currently, an estimated 99% of public-facing ProjectSend instances remain vulnerable. Active exploitation has been observed since September 2024, coinciding with the release of public exploits. Attackers are altering system settings, enabling user registration, and deploying webshells.

Vulnerability Details:

- **CVE-2024-11680**
- **Severity**: 9.8 CRITICAL
- Attackers can send specially crafted HTTP POST requests to the 'options.php' file, bypassing authentication and modifying the application's configuration
- This allows for:
  - Creation of unauthorized user accounts
  - Uploading of webshells
  - Embedding of malicious JavaScript

Affected Versions:

- ProjectSend versions prior to r1720

Fixed Version:

- ProjectSend version r1750

RECOMMENDATIONS:

Upgrade ProjectSend to fixed 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://nvd.nist.gov/vuln/detail/CVE-2024-11680