



مجلس الأمن السيبراني  
CYBER SECURITY COUNCIL



**Critical Vulnerability in LayerSlider WordPress Plugin**

Tracking #:432315750

Date:03-04-2024

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 INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a Critical Vulnerability in LayerSlider WordPress Plugin that could be exploited to gain unauthorized access to affected systems.

## TECHNICAL DETAILS:

### Vulnerability Details:

- **CVE-2024-2879**
- **CVSS Score: 9.8 (Critical)**
- A critical SQL injection vulnerability exists in LayerSlider WordPress Plugin. This vulnerability could be exploited by attackers to extract sensitive information from databases, including password hashes. An attacker could leverage this vulnerability to gain unauthorized access to a WordPress website.

### Affected Versions:

- LayerSlider versions 7.9.11 through 7.10.0

### Fixed Version:

- LayerSlider version 7.10.1

## RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by LayerSlider.

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.wordfence.com/blog/2024/04/5500-bounty-awarded-for-unauthenticated-sql-injection-vulnerability-patched-in-layerslider-wordpress-plugin/>
- <https://layerslider.com/release-log/>