مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in Everest Forms Plugin

Tracking #:432317574

Date:07-08-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in the Everest Forms plugin for WordPress, which could potentially be exploited to execute malicious code on affected systems.

TECHNICAL DETAILS:

Vulnerability Details:

- **Vulnerability ID**: CVE-2025-52709
- **Severity**: Critical (CVSS Score: **9.8**)
- The vulnerability arises from the plugin's handling of serialized data in form submissions. Specifically, the *evf_maybe_unserialize* function attempts to unserialize data when an admin views form entries in the WordPress dashboard.
- The vulnerable function is triggered via *column_form_field*, which renders form field data and calls *evf_maybe_unserialize*. A malicious actor can exploit this by submitting serialized payloads that instantiate arbitrary PHP objects, potentially leading to:
  - Remote Code Execution (RCE)
  - Data exfiltration
  - Full site compromise
- **Affected Versions**: Everest Forms **≤ 3.2.2**
- **Fixed Version**: Everest Forms **≥ 3.2.3**

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the fixed updates released by the Vendor.

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-2025-52709
- https://patchstack.com/articles/critical-vulnerability-impacting-over-100k-sites-patched-in-everest-forms-plugin/