مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in Everest Forms WordPress Plugin

Tracking #:432318765

Date:10-04-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability (CVE-2026-3296) with a CVSS score of 9.8 (Critical) has been identified in the Everest Forms WordPress Plugin, affecting 100,000+ websites.

TECHNICAL DETAILS:

A critical vulnerability (CVE-2026-3296) with a CVSS score of 9.8 (Critical) has been identified in the Everest Forms WordPress Plugin, affecting 100,000+ websites.
The flaw allows unauthenticated attackers to perform PHP Object Injection, potentially leading to remote code execution (RCE), full site compromise, and persistent backdoor installation.
The issue is actively exploitable via public-facing forms, requiring no authentication, making it highly dangerous for exposed environments.

Vulnerability Details

- CVE ID: CVE-2026-3296
- Severity: Critical (CVSS 9.8)
- Affected Software: Everest Forms WordPress Plugin ≤ v3.4.3
- Patched Version: v3.4.4
- Vulnerability Type: PHP Object Injection (Unsafe Deserialization)

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to update Everest Forms WordPress Plugin to fixed version or later 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://www.tenable.com/cve/CVE-2026-3296