مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Critical Vulnerability in W3 Total Cache
Tracking #:432318027
Date:18-11-2025

TLP: WHITE

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in the W3 Total Cache plugin that exposes WordPress websites to unauthenticated command injection. This flaw allows attackers to execute arbitrary PHP code simply by posting a malicious comment on websites running vulnerable versions of the plugin.

TECHNICAL DETAILS:

Vulnerability Description
- **CVE-2025-9501**
- **CVSS Score:** 9.0 Critical
- The issue stems from improper input handling within the plugin's internal _parse_dynamic_mfunc function. When processing user-submitted comments, the caching mechanism fails to sanitize dynamic input, allowing attackers to embed malicious PHP code that is executed when parsed.
- This flaw is trivially exploitable and requires no authentication or privileges, enabling remote attackers to trigger arbitrary code execution simply by posting a crafted comment on a vulnerable website.
- Successful exploitation can result in complete compromise of the affected site. An attacker may gain full control over the WordPress environment, access or steal sensitive data, deploy persistent backdoors or malware, deface the site, escalate privileges, or use the compromised system to conduct additional attacks.

Affected Versions
- W3 Total Cache < 2.8.13

Fixed Version
- W3 Total Cache 2.8.13 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided by 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://www.cve.org/CVERecord?id=CVE-2025-9501