مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in Greenshift WordPress Plugin

Tracking #:432317106

Date:22-04-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in the Greenshift WordPress plugin that could be exploited to execute malicious code, potentially leading to full website compromise.

TECHNICAL DETAILS:

A security vulnerability exists in the Greenshift WordPress plugin, tracked as CVE-2025-3616, this vulnerability allows authenticated users, even those with low privileges, to upload arbitrary files—including malicious PHP scripts—leading to remote code execution (RCE) and full site compromise.

Vulnerability Details:

- **CVE-2025-3616**
- **CVSS Score:** 8.8 (High)
- The flaw originates from the gspb_make_proxy_api_request() function, introduced in version 11.4, which added file upload capabilities. Due to insufficient validation, attackers can bypass MIME type checks and upload malicious webshells into a publicly accessible directory (/wp-content/uploads/api_upload/), enabling unauthorized execution of server commands.
- Exploitation of this vulnerability can lead to:
  - **Full website takeover**, allowing attackers unrestricted access.
  - **Data exfiltration**, defacement, or malicious script injection.
  - **Installation of backdoors**, leading to persistent threats.
  - **Privilege escalation**, granting unauthorized admin access.

Affected Versions:

- Greenshift – Animation and Page Builder Blocks v11.4 to v11.4.5

Fixed Versions:

- Greenshift v11.4.6 or later

RECOMMENDATIONS:

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

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-2025-3616