مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Actively exploited Remote Code Execution Vulnerability in Magento 2

Tracking #:432319068

Date:04-06-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical Remote Code Execution (RCE) vulnerability affecting Mirasvit Full Page Cache Warmer for Magento 2 has been identified and is currently being actively exploited in the wild.

TECHNICAL DETAILS:

A critical Remote Code Execution (RCE) vulnerability has been identified in Mirasvit Full Page Cache Warmer for Magento 2, tracked as CVE-2026-45247. The vulnerability arises from insecure deserialization of untrusted user-supplied data within the CacheWarmer cookie and has been assigned a CVSS v3.1 score of 9.8 (Critical).
The vulnerability is actively being exploited in the wild and has been added to Known Exploited Vulnerabilities (KEV) Catalog.

Vulnerability Details

- **Vulnerability:** Remote Code Execution (RCE) via PHP Object Injection
- **CVE ID:** CVE-2026-45247
- **Severity:** Critical
- **CVSS v3.1 Score:** 9.8 (Critical)
- **CVSS v4.0 Score:** 9.3 (Critical)
- **CWE:** CWE-502 – Deserialization of Untrusted Data
- **Affected Product:** Mirasvit Full Page Cache Warmer for Magento 2
- **Affected Versions:** All versions prior to 1.11.12
- **Patched Version:** 1.11.12 and later
- **Attack Vector:** Network
- **Authentication Required:** No
- **Privileges Required:** None
- **User Interaction Required:** No
- **Exploitation Status:** Actively exploited in the wild
- **Root Cause:** Insecure deserialization of user-controlled data from the CacheWarmer cookie using PHP's native unserialize() function.
- **Impact:** Allows unauthenticated attackers to execute arbitrary PHP code on the affected server.
- **Exploitation Method:** Attackers can send a crafted serialized PHP object within the CacheWarmer cookie, leveraging gadget chains available in Magento and its dependencies to achieve remote code execution.
- **Fix Availability:** Security patches released in version 1.11.12 (May 25, 2026), with additional stability improvements in version 1.11.13 (May 27, 2026).

RECOMMENDATIONS:

Immediate Actions:

- Organizations running vulnerable versions of Mirasvit Full Page Cache Warmer should prioritize remediation immediately due to active exploitation and the potential for unauthenticated remote code execution.

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://mirasvit.com/package/changelog/?package=mirasvit/module-cache-warmer