CYBER ADVISORY

Friday, January 16, 2026 **CAL-CSIC-202601-A-005**

Critical Remote Code Execution Vulnerability in Sitecore Products

UAT-8837	Exploited in the Wild	Remote Code Execution	CVE-2025-53690

Executive Summary:

The California Cybersecurity Integration Center (Cal-CSIC) has identified CVE-2025-53690, with a CVSS 3.1 score of 9.0, as a critical vulnerability affecting Sitecore Experience Platform (XP), Experience Manager (XM), and Experience Commerce (XC).[1] This advisory is being prioritized due to confirmed intelligence from Cisco Talos identifying the active exploitation of this vulnerability by UAT-8837, a Chinese state-sponsored threat group targeting North American critical infrastructure.[2]

UAT-8837 has been observed leveraging CVE-2025-53690 as a strategic entry point to establish long-term persistence within high-value networks. Successful exploitation allows unauthenticated remote code execution (RCE) via insecure deserialization. This CVE stems from a legacy configuration practice involving the use of insecure, publicly documented ASP.NET machine keys.

Cal-CSIC also validates the following indicators:

Indicator	Confirmation	Details
Proof of Concept (PoC) Published	YES	Public exploit scripts and Nuclei templates (e.g., GitHub Issue #13111) are available and circulated in the security community.[3]
Exploited in the Wild	YES	Confirmed exploitation by Chinese state-sponsored group UAT-8837 targeting critical infrastructure, as well as financially motivated groups distributing WEEPSTEEL malware.
CISA KEV Catalog	YES	Added to the CISA Known Exploited Vulnerabilities Catalog on September 4, 2025. Federal agencies are mandated to remediate by September 25, 2025.[4]

The Cal-CSIC recommends following security best practices in ASP.NET, including implementing automated machine key rotation, enabling View State Message Authentication Code (MAC), and encrypting any plaintext secrets within the web.config file.

For detailed Sitecore remediation instructions, refer to the official Sitecore advisory SC2025-005.[5]

References:

[1] Google; ViewState Deserialization Zero-Day Vulnerability in Sitecore Products (CVE-2025-53690); https://cloud.google.com/blog/topics/threat-intelligence/viewstate-deserialization-zero-day-vulnerability; accessed 16 January 2026

[2] Cisco Talos; UAT-8837 targets critical infrastructure sectors in North America; https://blog.talosintelligence.com/uat-8837/; accessed 16 January 2026

[3] Github; CVE-2025-53690 - Sitecore Experience Manager & Platform - Code Injection; https://github.com/projectdiscovery/nuclei-templates/issues/13111; accessed 16 January 2026

[4] CISA; CISA Adds Three Known Exploited Vulnerabilities to Catalog; https://www.cisa.gov/news-events/alerts/2025/09/04/cisa-adds-three-known-exploited-vulnerabilities-catalog; accessed 16 January 2026

[5] SITECORE Support; Security Bulletin SC2025-005; https://support.sitecore.com/kb?id=kb_article_view&sysparm_article=KB1003865; accessed 16 January 2026