مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Sitecore ViewState Deserialization Zero-Day Exploitation

Tracking #:432317671
Date-04-09-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed security researchers reported active exploitation of a ViewState deserialization zero-day vulnerability impacting Sitecore XP 9.0, Active Directory 1.4, and earlier deployments that reused sample machine keys from outdated Sitecore deployment guides (2017 and earlier).

TECHNICAL DETAILS:

An active exploitation of a ViewState deserialization zero-day vulnerability (**CVE-2025-53690**) is reported impacting Sitecore XP 9.0, Active Directory 1.4, and earlier deployments that reused sample machine keys from outdated Sitecore deployment guides (2017 and earlier).

Attackers leveraged these exposed ASP.NET machine keys to perform remote code execution (RCE) against internet-facing Sitecore instances. Successful exploitation enabled adversaries to establish persistence, escalate privileges, dump credentials, and perform Active Directory reconnaissance and lateral movement.

Mandiant observed attackers deploying custom malware (WEEPSTEEL), tunneling tools (EARTHWORM), remote access tools (DWAGENT), and AD reconnaissance frameworks (SharpHound). The exploitation campaign was disrupted, but the tactics confirm a sophisticated actor with deep product knowledge.

Organizations running Sitecore XP, XM, and XC deployments are at risk, especially if machine keys were left static or configured using public samples.

Key Findings:

- **Vulnerability:** ViewState deserialization (CVE-2025-53690) enabled by exposed machine keys.
- **Attack Vector:** Unauthenticated access to /sitecore/blocked.aspx endpoint with malicious __VIEWSTATE payloads.
- **Malware & Tools Observed:**
  - **WEEPSTEEL** – reconnaissance malware, disguised as ViewState payloads.
  - **EARTHWORM** – tunneling tool for SOCKS proxy.
  - **DWAGENT** – persistent remote access tool with SYSTEM privileges.
  - **SharpHound** – AD reconnaissance tool for BloodHound.
- **Persistence & Privilege Escalation:**
  - Creation of **local admin accounts** (asp$, sawadmin).
  - Use of **GoTokenTheft** for token impersonation.
  - Dumping of **SAM & SYSTEM hives** for credential theft.

Impacted Products:

Sitecore Products	Impact
Experience Manager (XM)	Potentially impacted
Experience Platform (XP)	
Experience Commerce (XC)	

Managed Cloud	Potentially impacted
XM Cloud	Not impacted
Content Hub	Not impacted
CDP and Personalize	Not impacted
OrderCloud	Not impacted
Storefront (formerly Four51 Storefront)	Not impacted
Send	Not impacted
Discover	Not impacted
Search	Not impacted
Commerce Server	Not impacted

RECOMMENDATIONS:

1. **Configuration Hardening**
   - Rotate and regenerate all **ASP.NET machine keys** in web.config.
   - Encrypt <machineKey> elements in configuration files.
   - Restrict access to web.config to application administrators only.
   - Disable/restrict exposure of /sitecore/blocked.aspx where possible.
2. **Detection & Response**
   - Review IIS logs for suspicious POST requests to /sitecore/blocked.aspx.
   - Monitor for **Event ID 1316 – ViewState verification failed** in Windows Application logs.
   - Investigate for presence of:
     - C:\Users\Public\Music\7za.exe
     - C:\Users\Public\Music\lfe.ico (EARTHWORM)
     - C:\Users\Public\Music\GoToken.exe
     - C:\Users\Public\Music\sh.exe (SharpHound)
   - Check for anomalous RDP logins and newly created local admin accounts (asp$, sawadmin).
3. **Network & Access Controls**
   - Block known malicious IPs:
     - 130.33.156[.]194
     - 103.235.46[.]102
   - Restrict outbound SOCKS proxy traffic and monitor for **EARTHWORM-like tunneling activity**.
   - Review Active Directory logs for enumeration commands (nltest, net group domain admins).
4. **Patching & Vendor Guidance**
   - Apply **Sitecore advisory SC2025-005** immediately.
   - Upgrade Sitecore deployments to **security-supported versions**.
   - Follow Microsoft's best practices for **ViewState MAC enforcement** and **ASP.NET key rotation**.

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://cloud.google.com/blog/topics/threat-intelligence/viewstate-deserialization-zero-day-vulnerability/
- https://support.sitecore.com/kb?id=kb_article_view&sysparm_article=KB1003865