Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Sitecore Zero-Day Powers Reconnaissance Malware

Date of Publication	Admiralty Code	TA Number
September 5, 2025	A1	TA2025271

Summary

Discovered On: September 2025
Affected Products: Sitecore Experience Manager (XM), Experience Platform (XP), and Experience Commerce (XC), Managed Cloud
Malware: WEEPSTEEL, EARTHWORM, DWAGENT, SHARPHOUND
Impact: A newly uncovered zero-day in Sitecore, CVE-2025-53690, is being actively exploited in the wild, giving attackers a direct path to run code on vulnerable servers. By abusing a hidden ViewState deserialization flaw, threat actors dropped the WEEPSTEEL malware to quietly map systems, steal configuration files, and dig deep into Active Directory. With clever use of fake admin accounts, tunneling tools, and stealthy persistence tricks, the attackers turned a small web flaw into full domain control, making this a reminder that even "hidden" features can open the door to major breaches.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-53690	Sitecore Multiple Products Deserialization of Untrusted Data Vulnerability	Sitecore Experience Manager (XM), Experience Platform (XP), and Experience Commerce (XC), Managed Cloud	✓	✓	✓

Vulnerability Details

#1

A critical zero-day in multiple Sitecore products, CVE-2025-53690, is being actively exploited in the wild. The flaw arises from a ViewState deserialization weakness, which can be abused to achieve remote code execution. Attackers are focusing on legacy Sitecore deployments, sending malicious HTTP requests to exploit a hidden ViewState form in legitimate components. These activities often left traces in event logs as "ViewState verification failed" messages, an early sign of compromise. Sitecore confirmed that newer deployments generate unique machine keys by default, greatly reducing risk, and said that impacted customers have already been notified.

#2 Once exploited, the servers decrypted attacker-supplied payloads that loaded a malicious .NET assembly dubbed WEEPSTEEL. This reconnaissance malware, similar to GhostContainer and ExchangeCmdPy.py, is designed to collect host, user, and network details, then exfiltrate them stealthily via hidden __VIEWSTATE fields in repeated HTTP POST requests. From the initial foothold, the attackers operated with IIS's NETWORK SERVICE privileges, which they leveraged to extract configuration files and further map the environment.

#3 The intrusion chain then expanded as adversaries staged additional tools. They dropped EARTHWORM, an open-source tunneler, to establish a reverse SOCKS proxy for command-and-control. Privilege escalation soon followed, with SYSTEM and ADMINISTRATOR access achieved through the creation of accounts like asp$ and sawadmin. These enabled RDP access, password hash theft, and registry hive dumping. They also deployed utilities such as DWAGENT, main.exe, and GoToken.exe, with DWAGENT playing a key role in maintaining SYSTEM-level persistence.

#4 To consolidate control, the attackers pivoted toward Active Directory reconnaissance. Using one of their newly created administrator accounts, they launched RDP sessions and executed SharpHound (sh.exe), BloodHound's data collection tool, to map AD trust relationships in detail. The collected intelligence was packaged for exfiltration, after which the attackers removed the asp$ and sawadmin accounts to cover their tracks. This incident highlights how a single overlooked flaw can quickly snowball into full domain compromise when combined with stealthy malware, privilege escalation, and systematic reconnaissance.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-53690	Sitecore Experience Manager (XM) and Experience Platform (XP) Through Version 9.0, Experience Commerce (XC), Managed Cloud, AD Version 1.4 and earlier	cpe:2.3:a:sitecore:experience_platform:*:*:*:*:*:*:*:*:* cpe:2.3:a:sitecore:experience_manager:*:*:*:*:*:*:*:*:* cpe:2.3:a:sitecore:experience_commerce:*:*:*:*:*:*:*:*:*	CWE-502

Recommendations

- **Update Sitecore immediately:** If you're running older or legacy Sitecore deployments, move to the latest version. Sitecore's modern builds generate a unique machine key automatically, which helps prevent this type of attack.
- **Rotate keys and credentials:** If your environment was exposed, assume the attackers may have stolen sensitive information. Change your machine keys, rotate admin and service account passwords, and review who has access to critical systems.
- **Check for suspicious accounts and tools:** Look for unexpected administrator accounts like asp$ or sawadmin, and scan for unusual files such as dwagent.exe, main.exe, or EARTHWORM that may have been planted by attackers.
- **Monitor your Active Directory and logs:** Keep a close eye on RDP sessions, password changes, and any unusual behavior in your event logs. Also, watch for "ViewState verification failed" errors, which could signal exploitation attempts.
- **Vulnerability Management:** This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third-party vendors, especially for critical applications and services.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence
TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0007 Discovery	TA0008 Lateral Movement
TA0010 Exfiltration	TA0011 Command and Control	T1588 Obtain Capabilities	T1588.006 Vulnerabilities

T1190 Exploit Public-Facing Application	**T1059** Command and Scripting Interpreter	**T1059.005** Visual Basic	**T1203** Exploitation for Client Execution
T1136 Create Account	**T1068** Exploitation for Privilege Escalation	**T1070** Indicator Removal	**T1082** System Information Discovery
T1027 Obfuscated Files or Information	**T1021** Remote Services	**T1021.001** Remote Desktop Protocol	**T1090** Proxy
T1105 Ingress Tool Transfer	**T1071** Application Layer Protocol	**T1071.001** Web Protocols	**T1041** Exfiltration Over C2 Channel
T1036 Masquerading			

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	117305c6c8222162d7246f842c4bb014, a39696e95a34a017be1435db7ff139d5, f410d88429b93786b224e489c960bf5c, be7e2c6a9a4654b51a16f8b10a2be175, 62483e732553c8ba051b792949f3c6d0, 63d22ae0568b760b5e3aabb915313e44
SHA256	a566cceaf9a66332470a978a234a8a8e2bbdd4d6aa43c2c75c25a80b3b744307, b3f83721f24f7ee5eb19f24747b7668ff96da7dfd9be947e6e24a688ecc0a52b, 61f897ed69646e0509f6802fb2d7c5e88c3e3b93c4ca86942e24d203aa878863
IPv4:Port	130[.]33[.]156[.]194[:]443, 130[.]33[.]156[.]194[:]8080, 103[.]235[.]46[.]102[:]80

Patch Details

Install the latest Sitecore updates or patches immediately to address the flaw.

Link: https://support.sitecore.com/kb?id=kb_article_view&sysparm_article=KB1003865

References

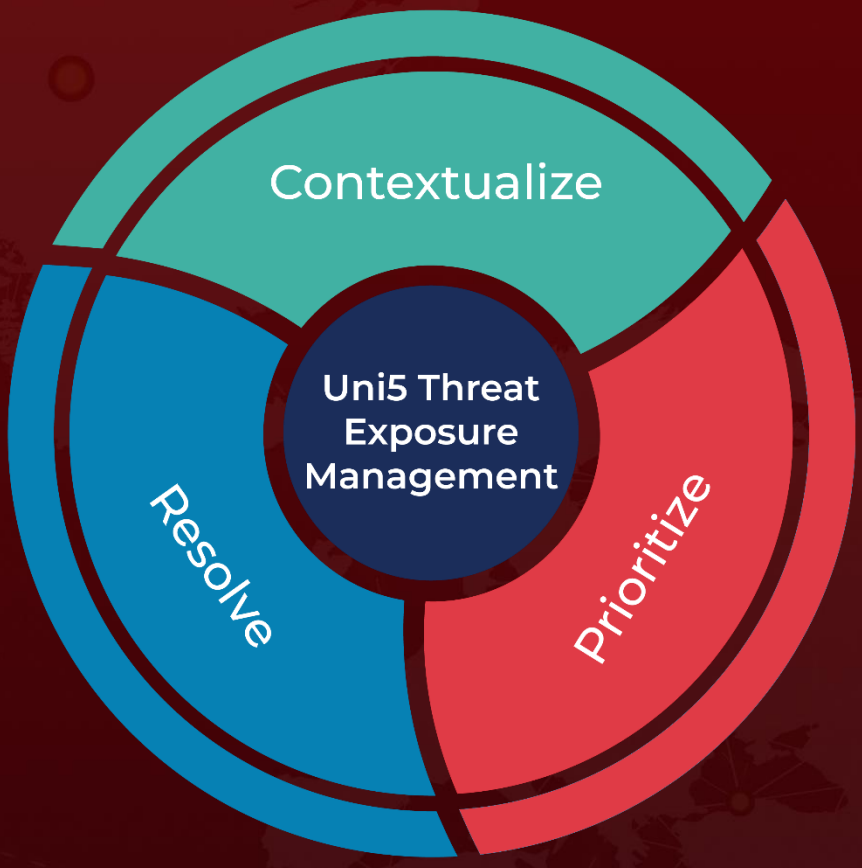
https://cloud.google.com/blog/topics/threat-intelligence/viewstate-deserialization-zero-day-vulnerability/

https://support.sitecore.com/kb?id=kb_article_view&sysparm_article=KB1003865

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

September 5, 2025 • 7:00 AM

More at www.hivepro.com