Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Critical Insecure Deserialization Vulnerability in Sitecore XM/XP

Date of Publication	Admiralty Code	TA Number
March 7, 2025	A1	TA2025069

Summary

First Seen: December 4, 2024
Affected Product: Sitecore Experience Manager (XM) and Experience Platform (XP)
Impact: CVE-2025-27218 is a critical security vulnerability identified in Sitecore Experience Manager (XM) and Experience Platform (XP) versions 10.4 and earlier. The vulnerability arises from an insecure deserialization flaw that allows an unauthenticated remote attacker to execute arbitrary code on the affected system. This could lead to full system compromise, data exfiltration, or further network penetration. With a public proof-of-concept (PoC) exploit now available, organizations are strongly urged to apply the official patch immediately.

⚙ CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-27218	Sitecore XM and XP Deserialization Vulnerability	Sitecore XM and XP	✗	✗	✓

Vulnerability Details

#1 CVE-2025-27218 is a critical security vulnerability identified in Sitecore Experience Manager (XM) and Experience Platform (XP) versions 10.4 and earlier. The vulnerability arises from an insecure deserialization flaw that allows an unauthenticated remote attacker to execute arbitrary code on the affected system.

#2 The vulnerability exists due to improper handling of serialized objects within Sitecore's platform. Attackers can craft and send malicious serialized objects to a vulnerable Sitecore instance, which, upon deserialization, leads to remote code execution. Exploiting this flaw requires no authentication, making it particularly dangerous in publicly exposed instances.

#3

The insecure deserialization occurs in a component responsible for handling user input, allowing attackers to inject arbitrary code execution payloads. If successfully exploited, this can result in complete server takeover, data breaches, service disruption, and unauthorized access to sensitive information. The availability of public proof-of-concept exploit further elevates the risk, making it imperative for organizations using vulnerable Sitecore versions to reassess their security posture immediately.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-27218	Sitecore Experience Manager (XM) and Experience Platform (XP) prior to 10.4 versions	cpe:2.3:a:sitecore:experience_manager:*:*:*:*:*:*:*:*	CWE-94

Recommendations

Apply Security Patches Immediately: Sitecore has released hotfixes to address this vulnerability. Users should apply the cumulative hotfix for version 10.4 as soon as possible. For container-based deployments, follow the official Sitecore documentation to ensure proper patching.

Implement Temporary Workarounds: If immediate patching is not possible, apply the Sitecore.Support.624693.config patch file as a temporary workaround. Place the patch file in the \App_Config\Include\zzz folder on Content Management (CM) and Standalone servers. Be aware that this workaround disables screenshot thumbnail functionality in Sitecore.

Restrict Public Access to Sitecore Instances: Limit exposure by ensuring Sitecore management interfaces and Content Management (CM) servers are not publicly accessible. Use firewall rules, VPNs, or allowlists to restrict access to trusted users only.

Monitor and Audit for Signs of Exploitation: Review logs for suspicious activity, such as unauthorized requests or unexpected deserialization attempts. Enable Intrusion Detection Systems (IDS) and Web Application Firewalls (WAF) to detect and block malicious payloads. Look for indicators of compromise (IoCs), including unauthorized system modifications.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0004 Privilege Escalation
T1059 Command and Scripting Interpreter	T1588 Obtain Capabilities	T1588.005 Exploits	T1068 Exploitation for Privilege Escalation
T1588.006 Vulnerabilities	T1190 Exploit Public-Facing Application	T1203 Exploitation for Client Execution	

Patch Details

Update Sitecore Experience Manager (XM) and Experience Platform (XP) to version 10.4 or later.

Links:
https://support.sitecore.com/kb?id=kb_article_view&sysparm_article=KB1003535

https://support.sitecore.com/kb?id=kb_article_view&sysparm_article=KB1003424

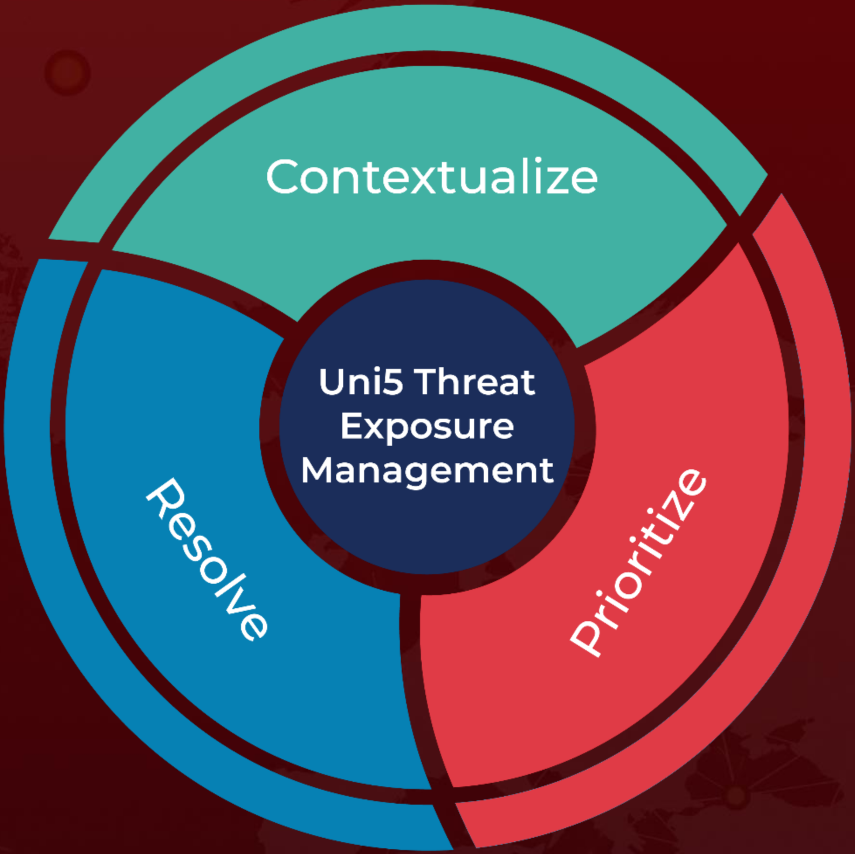
References

https://slcyber.io/blog/sitecore-unsafe-deserialization-again-cve-2025-27218

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

March 7, 2025 • 6:30 AM

More at www.hivepro.com