

Forum:[Hack Forums](#)

Thread: [Kentico Xperience CMS Authentication Bypass Vulnerability Allows Attackers to Execute](#)

JoseMar - March 19, 2025, 7:42 am

Kentico Xperience CMS Authentication Bypass Vulnerability Allows Attackers to Execute Arbitrary Code Remotely

Analysts found basic vulnerabilities in Kentico's Xperience CMS that may permit aggressors to compromise influenced frameworks.

The vulnerabilities, recognized as WT-2025-0006, WT-2025-0007, and WT-2025-0011, can be chained together to accomplish unauthenticated further code execution on frameworks with standard configurations.

Researchers at watchtower Labs recognized two unmistakable verification bypass vulnerabilities and one post-authentication inaccessible code execution imperfection.

These issues influence Kentico Xperience from 13 establishments with the Arranging Benefit empowered and designed to utilize username/password confirmation or maybe X.509 certificates.

Kentico Xperience CMS Verification Bypass Helplessness

To begin with, the confirmation bypass (WT-2025-0006) abuses a consistent blemish in how the CMS handles verification in its Organizing Benefit API.

By controlling Cleanser's demands to utilize secret word process verification with an uncommonly created username token, assailants can pick up regulatory get without substantial credentials.

A rearranged case of misuse includes sending a Cleanser ask with the following:

The moment confirmation bypass (WT-2025-0011) is indeed more concerning, requiring as it were a username with no watchword at all:

Once verified, aggressors can misuse the post-authentication RCE powerlessness (WT-2025-0007) by moving a way of traversal blemish in the media record transfer functionality.

This permits composing records to self-assertive areas on the server's filesystem.

The vulnerabilities stem from different issues:

To begin with, bypass happens when an invalid username is given; the framework returns a purge string instead of tossing an exception.

Combined with hash-based watchword confirmation, this makes a confirmation bypass.

The moment bypass misuses a consistent blemish in Microsoft's out-of-date Web Administrations Improvement 3.0 library, where the framework falls flat to approve tokens with the "SendNone" secret word option.

The RCE helplessness exists since the CheckAndEnsureFilePath strategy comes up short of appropriately approving record ways, permitting aggressors to type in records exterior expecting directories.

WatchTowr Labs Report states these vulnerabilities “can be insignificantly chained for RCE” and grant assailants “full control over the CMS.”

Kentico tended to these issues in a few updates: WT-2025-0006 was fixed in Kentico Xperience 13.0.173

WT-2025-0011 and WT-2025-0007 were fixed in Kentico Xperience 13.0.178

Security groups can confirm if their frameworks are helpless by utilizing discovery apparatuses distributed by watchtower on GitHub.

The analysts caution against utilizing Microsoft’s Web Administrations Improvement 3.0 library, expressing:

“Please, do not use the obsolete Microsoft Web Services Enhancement 3.0 for anything, you’ll get rekt.”

Organizations are emphatically prompted to promptly update the most recent form, particularly if utilizing username/password verification for the Arranging Benefit.

Don’t forget to update and stay safe!?

Additional sources to explore: You can also search directly by CVE on Google for more information:

<https://gbhackers.com/kentico-xperience-cms-vulnerability/>

<https://cybersecuritynews.com/kentico-authentication-bypass-vulnerability/>

<https://cyberpress.org/vulnerabilities-kentico/>