Overall Rating - High

BRITISH COLUMBIA

This notification is intended as an informational bulletin for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware of several vulnerabilities affecting various versions of Kentico CMS.

Technical Details

- In Kentico before 13.0.66, attackers can achieve Denial of Service via a crafted request to the GetResource handler. CVE-2022-32387

- Kentico CMS before 13.0.66 has an Insecure Direct Object Reference vulnerability. It allows an attacker with user management rights (default is Administrator) to export the user options of any user, even ones with higher privileges (like Global Administrators) than the current user. The exported XML contains every option of the exported user (even the hashed password). CVE-2022-29287

- Kentico Xperience 13.0.44 allows XSS via an XML document to the Media Libraries subsystem. CVE-2021-46163

- The Kentico Xperience CMS version 13.0 – 13.0.43 is vulnerable to a persistent Cross-Site Scripting (XSS) vulnerability (also known as Stored or Second Order XSS). Persistent XSS vulnerabilities occur when the application stores and retrieves client supplied data without proper handling of dangerous content. This type of XSS vulnerability is exploited by submitting malicious script content to the application which is then retrieved and executed by other application users. The attacker could exploit this to conduct a range of attacks against users of the affected application such as session hijacking, account take over and accessing sensitive data. CVE-2021-43991

- The Blog module in Kentico CMS 5.5 R2 build 5.5.3996 allows SQL injection via the tagname parameter. CVE-2021-27581

- Cross Site Scripting (XSS) vulnerability in Kentico before 12.0.75. CVE-2020-24794

- Kentico before 12.0.50 allows file uploads in which the Content-Type header is inconsistent with the file extension, leading to XSS. CVE-2019-19493

These vulnerabilities are rated as an overall **High** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.

- *Ensure mitigation is performed at your next change window.*

Please notify VRM with any questions or concerns you may have.

References

- CVE-2022-32387, CVE-2022-29287, CVE-2021-46163, CVE-2021-43991, CVE-2021-27581 CVE-2020-24794, CVE-2019-19493
- https://www.cvedetails.com/vulnerability-list/vendor_id-15688/Kentico.html