

Strapi CMS Vulnerability Exposes Sensitive Information in Admin Panel



A cleartext storage vulnerability in Strapi CMS allows attackers with admin panel access to discover sensitive user details through query filters, with potential for remote code execution when chained with another flaw.

- CVE-2023-22894 affects Strapi CMS, allowing exposure of sensitive user information through admin panel query filters
- The vulnerability stores sensitive information in cleartext, accessible to authenticated admin users
- Can be chained with CVE-2023-22621 to achieve remote code execution
- Affected product versions may be end-of-life or end-of-service
- Organizations are advised to discontinue use or transition to supported versions

Vulnerability Overview

Strapi, an open-source content management system, contains a **cleartext storage vulnerability** tracked as CVE-2023-22894. The flaw allows attackers who have gained access to the administrative panel to discover sensitive user details through the platform's query filter functionality. The vulnerability stems from the storage of sensitive information in an unencrypted format, making it accessible to authenticated users with administrative privileges.

The risk is compounded by the possibility of chaining this vulnerability with CVE-2023-22621, which could enable attackers to achieve **remote code execution** on affected systems. This escalation path significantly increases the potential impact on organizations running vulnerable Strapi instances.

Product Status and Mitigation

The affected Strapi versions may be end-of-life or end-of-service, meaning vendor support and security updates may no longer be available. Organizations currently using Strapi are strongly advised to evaluate their deployment status and consider discontinuing use of unsupported versions. Where continued operation is necessary, institutions should transition to supported versions that have addressed this vulnerability.

For regulated entities in the Kingdom, this vulnerability presents particular concern given the sensitivity of data typically managed through content management systems. The cleartext storage of sensitive information conflicts with data protection requirements and security baseline controls that mandate encryption of sensitive data at rest.

Risk Context

While the vulnerability requires existing administrative access, it represents a significant **privilege escalation** and information disclosure risk. In environments where multiple administrators operate with varying trust levels, or where administrative credentials may be compromised, the exposure of sensitive user details could facilitate further attacks or compliance violations.

What to do now

1. Identify all Strapi CMS instances deployed across your organization's infrastructure, including development, staging and production environments
2. Verify the version and support status of each Strapi deployment to determine if affected versions are end-of-life or end-of-service
3. Discontinue use of unsupported Strapi versions or migrate to current supported releases with security patches applied
4. Review administrative access logs for Strapi instances to identify any suspicious query filter activity or unauthorized information access
5. Implement additional access controls and monitoring for administrative panels, restricting access based

on least privilege principles

6. Assess whether any sensitive information may have been exposed and initiate incident response procedures if unauthorized access is suspected