

Path Traversal Vulnerability in ONLYOFFICE Docs Enables Remote Code Execution



A path traversal vulnerability in ONLYOFFICE Docs when JWT authentication is enabled allows attackers to upload malicious images and potentially execute remote code on affected servers.

- CVE-2021-3199 affects ONLYOFFICE Docs Server when JWT authentication is in use
- Attackers can exploit a path traversal flaw via `../` sequences in image upload parameters
- Successful exploitation may lead to remote code execution on the server
- Organizations must apply vendor mitigations or discontinue product use if patches are unavailable
- Internet-exposed instances require immediate assessment and remediation

Vulnerability Overview

ONLYOFFICE Docs Server contains a **path traversal vulnerability** tracked as CVE-2021-3199 that affects deployments using JWT authentication. The flaw allows attackers to manipulate image upload parameters by inserting `../` sequences, bypassing directory restrictions. This vulnerability creates a pathway for **remote code execution**, enabling attackers to run arbitrary commands on the server hosting the document collaboration platform.

The vulnerability specifically targets the image upload functionality when JWT tokens are configured for authentication. Attackers exploiting this weakness can traverse the file system structure, potentially placing malicious files in executable directories or overwriting critical system files.

Risk to Saudi Institutions

Regulated institutions in the Kingdom using ONLYOFFICE Docs for document collaboration face significant risk if their deployments are internet-accessible and have not applied vendor mitigations. Financial institutions, healthcare providers, and government entities that handle sensitive data through collaborative document platforms should prioritize assessment of their ONLYOFFICE installations.

The remote code execution capability means attackers could gain complete control over affected servers, potentially accessing confidential documents, customer data, or using compromised systems as pivot points for broader network intrusion.

Remediation Guidance

Organizations must immediately consult ONLYOFFICE vendor documentation for available security updates and apply them according to their change management procedures. Where mitigations are not available or cannot be applied promptly, institutions should consider isolating affected systems from internet access or discontinuing use until patches are deployed. All internet-facing ONLYOFFICE Docs instances require immediate inventory and risk assessment to determine exposure levels and prioritize remediation efforts.

What to do now

1. Identify all ONLYOFFICE Docs Server deployments within your environment, particularly those using JWT authentication
2. Assess internet exposure of each ONLYOFFICE instance and document external accessibility
3. Consult ONLYOFFICE vendor security bulletins for patches and apply updates through your change management process
4. If immediate patching is not feasible, isolate affected systems from internet access or implement network-level access controls
5. Review access logs for suspicious image upload activity or unusual file system traversal patterns

6. Consider discontinuing use of ONLYOFFICE Docs if vendor mitigations are unavailable and risk cannot be adequately contained