Docmosis Security Advisory: Arbitrary File Write in Tornado

Ref: DSA-2026-001
Product: Docmosis Tornado
Severity: Critical
CVSS: 9.1
Published: 20 August 2026
Last updated: 20 August 2026

Summary

Docmosis was notified of a vulnerability that uses the `storeTo=file` operation of the Tornado `/api/render` endpoint.

In affected versions, the file destination supplied to the render API is not sufficiently restricted. A caller who can access the Tornado API may be able to cause generated content to be written to unintended locations on the Tornado server.

For installations where no API Access Key has been configured, this may be exploitable without authentication. The vulnerability **does not** bypass Tornado API Access Key authentication.

The impact also depends on the operating system privileges assigned to the Tornado process. Docmosis deployment guidance specifies that Tornado should run under a basic user account and should not run as root or an administrative user. If Tornado is run with elevated operating system privileges, an arbitrary file write may have significantly greater impact, potentially including command execution with those privileges.

Affected Versions

- **Tornado 2.11.3 and earlier.**

Resolution

The vulnerability will be corrected in:

- **Tornado 2.11.4 and later. [Expected release date September 2026]**

Until then, customers using an affected version should apply the mitigations below.

Mitigation

Affected customers should immediately apply the following measures:

1. **Configure an API Access Key.** This requires callers to authenticate when accessing the Tornado API. The vulnerability **does not** bypass API Access Key authentication.
2. **Restrict access to the Tornado API** to trusted applications and networks.
3. **Run Tornado using a basic operating system user account.** Tornado should not run as root or an administrative user and should not be able to escalate privileges.

The recommendation to run Tornado with basic user privileges and to limit network access are already documented in the Tornado Deployment Security Guide.

Configuring an API Access Key and/or restricting network access to the Tornado API will prevent unauthorised exploitation of this vulnerability.

Running Tornado with basic user privileges also limits the potential impact of any successful exploitation.

Technical Details

Affected component: Tornado REST API `/api/render`
Affected option: `storeTo=file`
CWE: CWE-22 — Improper Limitation of a Pathname to a Restricted Directory

The `storeTo=file` option allows generated documents to be written to the local filesystem of the Tornado server.

In affected versions, insufficient validation of the supplied destination allows generated content to be written outside the intended location.

An attacker must be able to make requests to the Tornado API. Where an API Access Key has been configured, the attacker must also possess a valid key; this vulnerability does not bypass that authentication control.

The consequences of an arbitrary file write are determined by the operating system permissions of the account running Tornado. Where Tornado is run in accordance with the Deployment Security Guide, the process should have only basic user privileges. If Tornado is run with elevated privileges, the potential impact is correspondingly greater and may include remote command execution with those privileges.

CVSS

CVSS 3.1: 9.1 — Cirtical

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H

The CVSS score reflects an installation where the Tornado API is accessible without an API Access Key and where exploitation can result in high confidentiality, integrity and availability impact.

Acknowledgement

Docmosis thanks the security researcher who reported this vulnerability.

A technical analysis of the vulnerability has also been published by the researcher:

https://0day-rubbish.com/blog/docmosis-tornado-unauth-storeto-file-rce

Revision History

20 August 2026 — Initial advisory published.