CERT-EU

Security Advisory 2023-044

Path Traversal Vulnerability in Mastodon Media File Handler

July 7, 2023 — v1.0

TLP:CLEAR

Summary

A critical security vulnerability has been discovered in Mastodon versions up to 3.5.8/4.0.4/4.1.2. This vulnerability, identified as a path traversal issue, affects the Media File Handler component of Mastodon. Exploitation of this vulnerability could allow an attacker to create or overwrite any file that Mastodon has access to, potentially leading to Denial of Service (DoS) and arbitrary Remote Code Execution (RCE).

Technical Details

No additional technical details nor Proof of Concept is available at this time. This Security Advisory will be updated accordingly when the information is available.

Affected Products

Mastodon versions 3.5.0 and above up to 3.5.8/4.0.4/4.1.2 are affected by this vulnerability.

Recommendations

Users of affected versions are advised to upgrade to the patched versions immediately. The vulnerability has been fixed in the following versions:

- 4.1.3
- 4.0.5
- 3.5.9

References

[1] https://github.com/mastodon/mastodon/security/advisories/GHSA-9928-3cp5-93fm