> Vulnerability in GNU sed software _

20 April 2026 | CERT Polska(../../../../author/cert-polska/) | #vulnerability(../../../../tag/vulnerability/), #warning(../../../../tag/warning/), #cve(../../../../tag/cve/)

CVE ID	CVE-2026-5958(https://www.cve.org/CVERecord?id=CVE-2026-5958)
Publication date	20 April 2026
Vendor	GNU
Product	sed
Vulnerable versions	From 4.1e below 4.10
Vulnerability type (CWE)	Time-of-check Time-of-use (TOCTOU) Race Condition (CWE-367(https://cwe.mitre.org/data/definitions/367.html))
Report source	Report to CERT Polska

Description

CERT Polska has received a report about vulnerability in GNU sed software and participated in coordination of its disclosure.

The vulnerability CVE-2026-5958(https://www.cve.org/CVERecord?id=CVE-2026-5958): When sed is invoked with both `-i` (in-place edit) and `--follow-symlinks`, the function `open_next_file()` performs two separate, non-atomic filesystem operations on the same path: 1. resolves symlink to its target and stores the resolved path for determining when output is written, 2. opens the original symlink path (not the resolved one) to read the file. Between these two calls there is a race window. If an attacker

atomically replaces the symlink with a different target during that window, sed will: read content from the new (attacker-chosen) symlink target and write the processed result to the path recorded in step 1. This can lead to arbitrary file overwrite with attacker-controlled content in the context of the sed process.

This issue was fixed in version 4.10.

Credits

We thank Michał Majchrowicz and Marcin Wyczechowski (AFINE Team) for the responsible vulnerability report.

More about the coordinated vulnerability disclosure process at CERT Polska can be found at https://cert.pl/en/cvd/(https://cert.pl/en/cvd/).

CERT Polska is a team operating within the structures of NASK - National Research Institute, established in 1996 to respond to computer security incidents. It carries out the role of CSIRT NASK, one of three such teams operating at the national level within the Polish national cybersecurity system.

Social media

Facebook(https://www.facebook.com/CERT.Polska/)

X(https://x.com/CERT_Polska_en)

LinkedIn(https://www.linkedin.com/showcase/cert-polska)

GitHub(https://github.com/CERT-Polska)

Contact

Address: Kolska 12, 01-045 Warsaw, Poland
ePUAP: /NASK-Instytut/SkrytkaESP
e-Doręczenia: AE:PL-60057-61611-BCEGR-11

E-mail: info@cert.pl(mailto:info@cert.pl)
Incident reporting: incydent.cert.pl(https://incydent.cert.pl/#!/lang=en)
cert@cert.pl(mailto:cert@cert.pl)

Co-financed by the Connecting Europe Facility of the European Union