> Vulnerabilities in Ollama software _

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

CVE ID	CVE-2026-42248(https://www.cve.org/CVERecord?id=CVE-2026-42248)
Publication date	29 April 2026
Vendor	Ollama
Product	Ollama
Vulnerable versions	From 0.12.10 through 0.17.5
Vulnerability type (CWE)	Download of Code Without Integrity Check (CWE-494(https://cwe.mitre.org/data/definitions/494.html))
Report source	Report to CERT Polska

CVE ID	CVE-2026-42249(https://www.cve.org/CVERecord?id=CVE-2026-42249)
Publication date	29 April 2026
Vendor	Ollama
Product	Ollama
Vulnerable versions	From 0.12.10 through 0.17.5

Vulnerability type (CWE)	Download of Code Without Integrity Check Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') (CWE-494 22(https://cwe.mitre.org/data/definitions/494 22.html))
Report source	Report to CERT Polska

Description

CERT Polska has received a report about vulnerabilities in Ollama software and participated in coordination of their disclosure.

The vulnerability CVE-2026-42248(https://www.cve.org/CVERecord?id=CVE-2026-42248): Ollama for Windows does not perform integrity or authenticity verification of downloaded update executables. Unlike other platforms, the Windows implementation of the update verification routine unconditionally returns success so no digital signature or trust validation is performed before staging or executing update payloads, enabling attacker-supplied executables to be accepted and later executed by the application.

Critically, Ollama for Windows performs silent automatic updates, so the malicious payload may be installed automatically without user awareness.

The vulnerability CVE-2026-42249(https://www.cve.org/CVERecord?id=CVE-2026-42249): Ollama for Windows contains a Remote Code Execution vulnerability in its update mechanism due to improper handling of attacker-controlled HTTP response headers. When downloading updates, the application constructs local file paths using values derived from HTTP headers without validation. These values are passed directly to `filepath.Join`, allowing path traversal sequences (../) to be resolved and enabling files to be written outside the intended update staging directory. An attacker who can influence update responses can exploit this flaw to write arbitrary executables to attacker-chosen locations accessible to the current user, including the Windows Startup directory. This allows execution of arbitrary executables.

Critically, when chained with CVE-2026-42248 (Missing Signature Verification for Updates), an attacker can deliver malicious payloads that are written to sensitive locations and executed automatically. Because Ollama for Windows performs silent automatic updates and executes staged binaries without user interaction, this results in automatic and persistent code execution without user awareness.

Maintainers of this project were notified early about these vulnerabilities, but didn't respond with the details of vulnerabilities or vulnerable version range. Versions from 0.12.10 to 0.17.5 were tested and confirmed as vulnerable, other versions were not tested but might also be vulnerable.

Credits

We thank Bartłomiej Dmitruk (striga.ai) 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/).

Report an incident(https://incydent.cert.pl/#/lang=en)

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-26

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