> Vulnerability in Bludit software _

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

CVE ID	CVE-2026-4420(https://www.cve.org/CVERecord?id=CVE-2026-4420)
Publication date	07 April 2026
Vendor	Bludit
Product	Bludit
Vulnerable versions	3.17.2, 3.18.0
Vulnerability type (CWE)	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') (CWE-79(https://cwe.mitre.org/data/definitions/79.html))
Report source	Report to CERT Polska

Description

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

The vulnerability CVE-2026-4420(https://www.cve.org/CVERecord?id=CVE-2026-4420): Bludit is vulnerable to Stored Cross-Site Scripting (XSS) in its page creating functionality. An authenticated attacker with page creation privileges (such as Author, Editor, or Administrator) can embed a malicious JavaScript payload in the tags field of a newly created article. This payload will be executed when a

victim visits the URL of the uploaded resource. The uploaded resource itself is accessible without authentication. Critically, this vulnerability could be used to automatically create a new site administrator if the victim has enough privileges.

The vendor was notified early about this vulnerability, but didn't respond with the details of vulnerability or vulnerable version range. Only versions 3.17.2 and 3.18.0 were tested and confirmed as vulnerable, other versions were not tested and might also be vulnerable.

Credits

We thank Yassin Abdelrazek 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