

(/en/).

Report an incident(<https://www.cert.pl/#/add-incident>)

([../..](#)) (/en/s
[../p](#) [earc](#)
[osts/](#) [h](#)).
[2026](#)
[/01/](#)
[CVE-](#)
[2025](#)
[-459](#)
[6/](#)).

> Vulnerability in Asseco AMDX software

08 January 2026 | [CERT Polska](#) | [#vulnerability](#), [#warning](#), [#cve](#).

CVE ID	CVE-2025-4596
Publication date	08 January 2026
Vendor	Asseco
Product	AMDX
Vulnerable versions	All before 6.09.01.62
Vulnerability type (CWE)	Authorization Bypass Through User-Controlled Key (CWE-639)
Report source	Report to CERT Polska

Description

Asseco ADMX software is a hospital information system (HIS) used for processing medical records. CERT Polska has received a report about vulnerability in ADMX software and participated in coordination of its disclosure.

The vulnerability [CVE-2025-4596](https://www.cve.org/CVERecord?id=CVE-2025-4596) allows logged in patients to access medical files belonging to other patients through manipulation of GET arguments containing document IDs. This issue has been fixed in 6.09.01.62 version of ADMX.

Credits

We thank Wiktor Mróz 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/>).

Social media

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.

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>)

<https://cert.pl/en/s>
<https://cert.pl/en/s>
<https://cert.pl/en/s>
<https://cert.pl/en/s>

2026
Contact
<https://cert.pl/en/s>

Address: Kolska 12, 01-045 Warsaw, Poland
ePUAP: /NASK-Institut/SkrytkaESP
e-Doręczenia: AEPL-60057-61611-BCEGR-
2025
-459

6/)

E-mail: info@cert.pl (<mailto:info@cert.pl>).

Incident reporting:

[incydent.cert.pl](https://incydent.cert.pl/#!/lang=en) (<https://incydent.cert.pl/#!/lang=en>).

cert@cert.pl (<mailto:cert@cert.pl>).



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