> Vulnerabilities in Asseco InfoMedica Plus software _

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

CVE ID	CVE-2025-8306(https://www.cve.org/CVERecord?id=CVE-2025-8306)
Publication date	08 January 2026
Vendor	Asseco
Product	InfoMedica Plus
Vulnerable versions	From 4.0.0 to 4.50.1 and from 5.0.0 to 5.38.0
Vulnerability type (CWE)	Insufficient Granularity of Access Control (CWE-1220(https://cwe.mitre.org/data/definitions/1220.html))
Report source	Report to CERT Polska

CVE ID	CVE-2025-8307(https://www.cve.org/CVERecord?id=CVE-2025-8307)
Publication date	08 January 2026
Vendor	Asseco
Product	InfoMedica Plus
Vulnerable versions	From 4.0.0 to 4.50.1 and from 5.0.0 to 5.38.0
Vulnerability type (CWE)	Storing Passwords in a Recoverable Format (CWE-257(https://cwe.mitre.org/data/definitions/257.html))

Description

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

Asseco InfoMedica is a comprehensive solution used to manage both administrative and medical tasks in the healthcare sector.

The vulnerability CVE-2025-8306(https://www.cve.org/CVERecord?id=CVE-2025-8306): A low privileged user is able to obtain encoded passwords of other accounts (including main administrator) due to lack of granularity in access control. The vulnerability CVE-2025-8307(https://www.cve.org/CVERecord?id=CVE-2025-8307): Passwords of all users are stored in a database in an encoded format. An attacker in possession of these encoded passwords is able to decode them by using an algorithm embedded in the client-side part of the software.

Chained exploitation of these vulnerabilities allows an attacker to escalate privileges.

Both vulnerabilities have been fixed in versions **4.50.1** and **5.38.0**

Credits

We thank Maciej Kazulak 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/).

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