



Hardcoded credentials in Comarch ERP Optima

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

| | |
|------------------------|---|
| CVE | CVE-2025-68421 |
| State | PUBLISHED |
| Assigner | CERT-PL |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2026-05-14 11:16:17 UTC |
| Updated | 2026-05-14 11:16:17 UTC |
| Description | Comarch ERP Optima client makes use of a hard-coded password for a database user. These credentials cannot be chang |

Risk And Classification

Primary CVSS: v4.0 8.7 HIGH from cvd@cert.pl

CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:L/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Problem Types: CWE-798 | CWE-798 CWE-798 Use of Hard-coded Credentials

| Version | Source | Type | Score | Severity | Vector |
|---------|-------------|-----------|-------|----------|--|
| 4.0 | cvd@cert.pl | Secondary | 8.7 | HIGH | CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:L/SC:N/SI:N/SA:N/E:X/C... |
| 4.0 | CNA | CVSS | 8.7 | HIGH | CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:L/SC:N/SI:N/SA:N |

CVSS v4.0 Breakdown

Attack Vector

Adjacent

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

High

Availability

Low

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:L/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX:MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|--------|-------------------------|----------------------------|------------------------|---------------|
| CNA | Comarch | ERP Optima | affected 2026.4 custom | Not specified |

References

| Reference | Source | Link | Tags |
|--|-----------------------------|--------------------------------|---------------------|
| cert.pl/posts/2026/05/CVE-2025-68420 | cvd@cert.pl | cert.pl | |
| www.comarch.pl/erp/comarch-optima | cvd@cert.pl | www.comarch.pl | |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, analysis |

Vendor Comments And Credit

Discovery Credit

CNA: Wojciech Giełda (en)

Additional Advisory Data

Workarounds

CNA: Since these accounts are used for backward compatibility only, in some cases it is possible to disable them in the SQL server.

There are currently no legacy QID mappings associated with this CVE.

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report