

(/).

Ostrzeżenia(<https://moje.cert.pl/komunikaty/>).

Złóż zgłoszenie(<https://moje.cert.pl/zloz-zgloszenie/>).

([../..](#) ([/szu](#)  
[../en/](#) [kaj](#)).

[post](#)

## > Podatności w oprogramowaniu DobryCMS/20

02 marca 2026 | [CERT Polska](#)([../..../author/cert-polska/](#)) | [#podatność](#)([../..../tag/podatnosc/](#)),  
[#ostrzezenie](#)([../..../tag/ostrzezenie/](#)), [#cve](#)([../..../tag/cve/](#)).

[26/0](#)

[3/CV](#)

[E-](#)

[2025](#)

<b>CVE ID</b>	<a href="https://www.cve.org/CVERecord?id=CVE-2025-12462">CVE-2025-12462</a> ( <a href="https://www.cve.org/CVERecord?id=CVE-2025-12462">https://www.cve.org/CVERecord?id=CVE-2025-12462</a> )	<a href="#">-12462/</a>
<b>Data publikacji</b>	02 marca 2026	
<b>Producent podatnego oprogramowania</b>	Studio Fabryka	
<b>Nazwa podatnego oprogramowania</b>	DobryCMS	
<b>Podatne wersje</b>	Do 8.0	
<b>Typ podatności (CWE)</b>	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') ( <a href="https://cwe.mitre.org/data/definitions/89.html">CWE-89</a> ( <a href="https://cwe.mitre.org/data/definitions/89.html">https://cwe.mitre.org/data/definitions/89.html</a> ))	
<b>Źródło zgłoszenia</b>	Zgłoszenie do CERT Polska	
<b>CVE ID</b>	<a href="https://www.cve.org/CVERecord?id=CVE-2025-14532">CVE-2025-14532</a> ( <a href="https://www.cve.org/CVERecord?id=CVE-2025-14532">https://www.cve.org/CVERecord?id=CVE-2025-14532</a> )	
<b>Data publikacji</b>	02 marca 2026	
<b>Producent podatnego oprogramowania</b>	Studio Fabryka	

Nazwa podatnego oprogramowania	DobryCMS
Podatne wersje	Od 1.0 do 1.* włącznie Od 2.0 do 2.* włącznie 5.0
Typ podatności (CWE)	Unrestricted Upload of File with Dangerous Type (CWE-434( <a href="https://cwe.mitre.org/data/definitions/434.html">https://cwe.mitre.org/data/definitions/434.html</a> ))
Źródło zgłoszenia	Zgłoszenie do CERT Polska

## Opis podatności

CERT Polska otrzymał zgłoszenie o podatnościach w oprogramowaniu DobryCMS. Skoordinował proces ujawniania informacji.

Podatność [CVE-2025-12462](https://www.cve.org/CVERecord?id=CVE-2025-12462): W DobryCMS zidentyfikowano podatność typu Blind SQL Injection. Zdalny, nieuwierzytelniony atakujący może wstrzykiwać dowolne kwerendy w języku SQL w ścieżce URL w wielu parametrach.

Ten problem zostały naprawiony w wersjach powyżej 8.0.

Podatność [CVE-2025-14532](https://www.cve.org/CVERecord?id=CVE-2025-14532): Funkcjonalność przesyłania plików w DobryCMS umożliwia zdalnemu, nieuwierzytelnionemu atakującemu przesyłanie plików dowolnego typu i z dowolnym rozszerzeniem bez jakichkolwiek ograniczeń, co może prowadzić do zdalnego wykonania kodu.

Ten problem zostały naprawiony w wersjach powyżej 5.0.

## Podziękowania

Za zgłoszenie podatności Blind SQL Injection dziękujemy Jarosławowi Wieczorkowi, Pawłowi Berusowi, Kacprowi Gendoszowi oraz Karolinie Buchnat. Natomiast za zgłoszenie dotyczące podatności Unrestricted File Upload dziękujemy Dawidowi Radzińskiemu z RED SECURITY.

Więcej o procesie zgłaszania podatności można przeczytać na stronie <https://cert.pl/cvd/>.

CERT Polska  
w social mediach

Facebook(<https://www.facebook.com/cert.pl>)

Kontakt

ul. Kolska 12, 01-045 Warszawa  
ePUAP: /NASK-Institut/SkrytkaESP

e-Doręczenia: AE:PL-60057-61611-BCEGR-

(/)

CERT Polska to zespół działający w strukturach NASK - Państwowego Instytutu Badawczego, powołany w 1996 roku do reagowania na incydenty bezpieczeństwa komputerowego. Realizuje zadania

cebook.com/CERT.Polska /)

e-mail: [info@cert.pl](mailto:info@cert.pl)(mailto:info@cert.pl),  
Zgłaszanie incydentów:  
[incydent.cert.pl](mailto:incydent.cert.pl)(https://incydent.cert.pl/),  
[cert@cert.pl](mailto:cert@cert.pl)(mailto:cert@cert.pl).

**Ostrzeżenia**(<https://moje.cert.pl/komunikaty/>).

CSIRT NASK, jednego z trzech takich zespołów działających na poziomie krajowym w ramach krajowego systemu cyberbezpieczeństwa.

LinkedIn(<https://www.linkedin.com/showcase/cert-polska>)

GitHub(<https://github.com/CERT-Polska>)

(././././) (/szu  
././en/ kaj).

post  
s/20  
26/0



**Współfinansowane przez instrument Unii Europejskiej „Łącząc Europę”**

3/CV  
E-

© 2026 NASK(<https://nask.pl/>) | Polityka prywatności(<https://nask.pl/uploads/misc/privacy-policy.pdf>) |

Deklaracja dostępności(<https://nask.pl/deklaracja-dostepnosc/>) | CSIRT GOV(<https://csirt.gov.pl/>) |

CSIRT MON(<https://csirt-mon.wp.mil.pl/>).

2025  
124  
62/).