

(/).

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

Zgłoś Incident(<https://incident.cert.pl/>)

(../.. (/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

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

Nazwa podatnego oprogramowania	DobryCMS
Podatne wersje	Od 1.0 do 1.* włącznie Od 2.0 do 2.* włącznie 5.0
Ostrzeżenia	(https://moje.cert.pl/komunikaty/)
Typ podatności (CWE)	Unrestricted Upload of File with Dangerous Type (CWE-434(https://cwe.mitre.org/data/definitions/434.html))
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 został 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 został 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/certpolska>)

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 /)

11

e-mail: info@cert.pl(mailto:info@cert.pl).

Zgłaszanie incydentów:

incydent.cert.pl(https://incydent.cert.pl/).

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>)



Współfinansowane przez instrument Unii Europejskiej „Łącząc Europę”

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

[Deklaracja dostępności](#)(/deklaracja-dostepnosci/) | CSIRT GOV(<https://csirt.gov.pl/>) |

[CSIRT MON](https://csirt-mon.wp.mil.pl/)(https://csirt-mon.wp.mil.pl/).

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

post

s/20

26/0

3/CV

E-

2025

124

62/).