> Podatności w oprogramowaniu Hydrosystem Control System _

09 kwietnia 2026 | CERT Polska(../../../../author/cert-polska/) | #podatność(../../../../tag/podatnosc/), #ostrzeżenie(../../../../tag/ostrzezenie/), #cve(../../../../tag/cve/)

CVE ID	CVE-2026-4901(https://www.cve.org/CVERecord?id=CVE-2026-4901)
Data publikacji	09 kwietnia 2026
Producent podatnego oprogramowania	Hydrosystem
Nazwa podatnego oprogramowania	Control System
Podatne wersje	Wszystkie poniżej 9.8.5
Typ podatności (CWE)	Insertion of Sensitive Information into Log File (CWE-532(https://cwe.mitre.org/data/definitions/532.html))
Źródło zgłoszenia	Zgłoszenie do CERT Polska

CVE ID	CVE-2026-34184(https://www.cve.org/CVERecord?id=CVE-2026-34184)
Data publikacji	09 kwietnia 2026
Producent podatnego oprogramowania	Hydrosystem

Nazwa podatnego oprogramowania	Control System
Podatne wersje	Wszystkie poniżej 9.8.5
Typ podatności (CWE)	Missing Authorization (CWE-862(https://cwe.mitre.org/data/definitions/862.html))
Źródło zgłoszenia	Zgłoszenie do CERT Polska

CVE ID	CVE-2026-34185(https://www.cve.org/CVERecord?id=CVE-2026-34185)
Data publikacji	09 kwietnia 2026
Producent podatnego oprogramowania	Hydrosystem
Nazwa podatnego oprogramowania	Control System
Podatne wersje	Wszystkie poniżej 9.8.5
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

Opis podatności

CERT Polska otrzymał zgłoszenie o podatnościach w oprogramowaniu Hydrosystem Control System i koordynował proces ujawniania informacji.

Podatność CVE-2026-4901(https://www.cve.org/CVERecord?id=CVE-2026-4901): Hydrosystem Control System zapisuje wrażliwe informacje w pliku z logami. Co istotne, dane uwierzytelniające użytkownika także są zapisywane w logu, co umożliwia atakującemu uzyskanie dalszego autoryzowanego dostępu do systemu. W połączeniu z podatnością CVE-2026-34184, te wrażliwe informacje mogą być uzyskiwane przez nieautoryzowanego użytkownika.

Podatność CVE-2026-34184(https://www.cve.org/CVERecord?id=CVE-2026-34184): Hydrosystem Control System nie wymusza autoryzacji dla niektórych katalogów. To umożliwia nieautoryzowanemu atakującemu odczytywanie wszystkich plików w tych katalogach oraz ich wykonywanie. Co istotne, atakujący może bezpośrednio uruchomić skrypty PHP wykonujące operacje na połączonej bazie danych.

Podatność CVE-2026-34185(https://www.cve.org/CVERecord?id=CVE-2026-34185): Hydrosystem Control System jest podatny na SQL Injection w większości skryptów i parametrów wejściowych. Ponieważ nie zastosowano żadnych mechanizmów ochronnych, uwierzytelniony atakujący może wstrzyknąć dowolne polecenie SQL, co może prowadzić do uzyskania pełnej kontroli nad bazą danych.

Te problemy zostały naprawione w wersji 9.8.5

Podziękowania

Za zgłoszenie podatności dziękujemy Jarosławowi "Jahrek" Kamińskiemu - Securitum.

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

CERT Polska to zespół działający w strukturach NASK - Państwowego Instytutu Badawczego, powołany w 1996 roku do reagowania na incydenty bezpieczeństwa komputerowego. Realizuje zadania CSIRT NASK, jednego z trzech takich zespołów działających na poziomie krajowym w ramach krajowego systemu cyberbezpieczeństwa.

CERT Polska w social mediach

Facebook(https://www.facebook.com/CERT.Polska/)

X(https://x.com/CERT_Polska)

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

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

Kontakt

ul. Kolska 12, 01-045 Warszawa
ePUAP: /NASK-Instytut/SkrytkaESP
e-Doręczenia: AE:PL-60057-61611-BCEGR-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)

Współfinansowane przez instrument Unii Europejskiej „Łącząc Europę”