

WRZESIEŃ 2026

Podsumowanie Miesiąca CERT POLSKA

Nr 9/2026

PODSUMOWANIE MIESIĄCA CERT POLSKA



PROJEKT FINANSOWANY ZE ŚRODKÓW
MINISTERSTWA CYFRYZACJI

TLP: CLEAR

Publikacja wyraża jedynie poglądy autora/ów i nie może być utożsamiana z oficjalnym stanowiskiem Ministerstwa Cyfryzacji.

Autor: zespół CERT Polska

© Państwowy Instytut Badawczy NASK

Publikacja jest rozpowszechniana na zasadach licencji Creative Commons.

Uznanie autorstwa (CC BY) 4.0 Międzynarodowe.

SPIS TREŚCI

Statystyki zgłoszonych zagrożeń oraz zarejestrowanych incydentów	4
Moje.cert.pl	9
Podatności CVE	10
Wybrane podatności i ich wpływ na krajobraz cyberbezpieczeństwa w Polsce – IX 2026	10
Wybrane informacje	13
Wystąpienia ekspertów CERT Polska	16
Komunikaty o zagrożeniach	17
Opis najczęściej występujących kampanii – IX 2026	21

Statystyki zgłoszonych zagrożeń oraz zarejestrowanych incydentów

Zgłoszenia i incydenty cyberbezpieczeństwa

Statystyki przedstawione w tym rozdziale obejmują dane o liczbie zgłoszeń¹ oraz o liczbie incydentów obsługiwanych przez CSIRT NASK w okresie od 1 do 30 września 2026 r. Wybrane dane ujęto również w szerszym horyzoncie czasowym, aby umożliwić obserwację zmian zachodzących w dłuższym okresie.

W dniu 3 kwietnia 2026 r. weszła w życie nowelizacja ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (UoKSC), która zmieniła definicje ustawowe, wprowadziła nowe kategorie podmiotów – podmioty kluczowe oraz podmioty ważne – a także rozszerzyła zakres raportowania o potencjalne zdarzenia dla cyberbezpieczeństwa (art. 2 pkt 11e), cyberzagrożenia (art. 2 pkt 4a) oraz poważne cyberzagrożenia (art. 2 pkt 11f). Nowelizacja zmodyfikowała również zasady klasyfikacji incydentów oraz poszerzyła katalog sektorów i podmiotów objętych ustawą. W konsekwencji dane publikowane od kwietnia 2026 r. mogą nie być w pełni porównywalne z danymi z okresów wcześniejszych.

Zgłoszone zagrożenia oraz zarejestrowane incydenty – IX 2026

Tabela 1. Liczba zgłoszeń oraz zarejestrowanych incydentów od 1 do 30 września 2026 r.

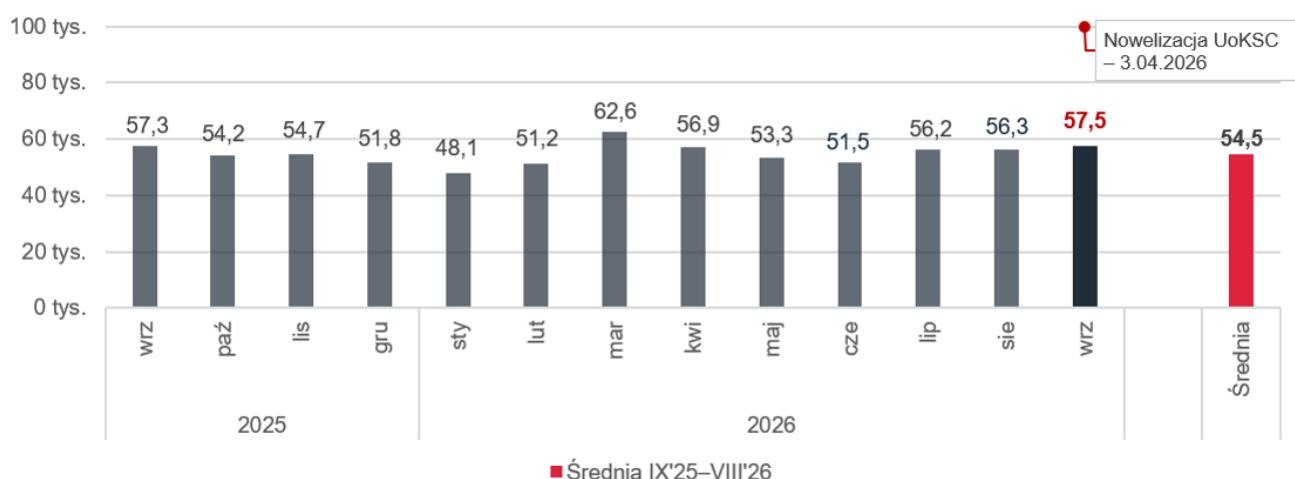
Zgłoszone zagrożenia i zarejestrowane incydenty	Liczba
Zgłoszenia potencjalnych zdarzeń dla cyberbezpieczeństwa*	5,6 tys.
Zgłoszenia cyberzagrożeń*	49,1 tys.
Zgłoszenia incydentów	2,8 tys.
Zgłoszenia poważnych cyberzagrożeń*	0,03 tys.
Razem zgłoszenia	57,5 tys.
Zarejestrowane incydenty**	19,2 tys.

* Nowe kategorie zgłoszeń raportowane od kwietnia 2026 r. ** Incydenty zostały zarejestrowane na podstawie zgłoszeń incydentów, zgłoszeń cyberzagrożeń, zgłoszeń poważnych cyberzagrożeń oraz zgłoszeń potencjalnych zdarzeń dla cyberbezpieczeństwa.

¹ Zgłoszenia przesyłane są za pośrednictwem formularza dostępnego na stronie <https://incydent.cert.pl> lub są wysyłane na adres zgłoszeniowy cert@cert.pl, a także poprzez system S46. Otrzymane informacje o zagrożeniach stanowią podstawę rejestracji nowych incydentów.

We wrześniu 2026 r. zespół CERT Polska otrzymał **łącznie 57,5 tys. zgłoszeń**. Na ich podstawie **zarejestrowano 19,2 tys. incydentów** cyberbezpieczeństwa, które miały lub mogły mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych. Dotyczą one konkretnych kategorii zagrożeń, np. szkodliwych stron wyludzających poufne informacje (ang. *phishing*), spamu czy ataku z użyciem szkodliwego oprogramowania. W wielu przypadkach jeden incydent był powiązany z kilkoma zgłoszeniami.

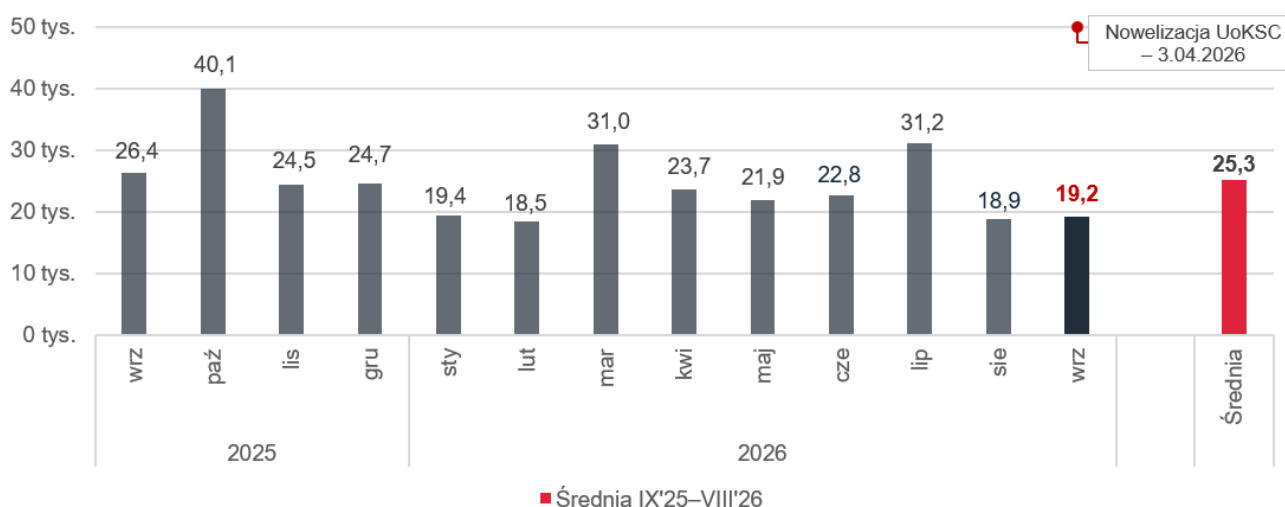
Zgłoszenia zagrożeń od IX 2025 do IX 2026



Wykres 1. Liczba wszystkich zgłoszeń od 01.09.2025 do 30.09.2026. Źródło: CERT Polska / CSIRT NASK.

Liczba wszystkich zgłoszeń odnotowanych we wrześniu 2026 r. utrzymywała się powyżej średniej z poprzednich 12 miesięcy. W porównaniu z analogicznym miesiącem 2025 r. liczba ta pozostawała na zbliżonym poziomie, natomiast w stosunku do sierpnia 2026 r. **wzrosła o 2%**.

Zarejestrowane incydenty cyberbezpieczeństwa od IX 2025 do IX 2026



Wykres 2. Liczba zarejestrowanych incydentów od 01.09.2025 do 30.09.2026. Źródło: CERT Polska / CSIRT NASK.

Liczba incydentów zarejestrowanych we wrześniu 2026 r. wyniosła **19,2 tys.** W porównaniu z analogicznym miesiącem 2025 r. **była niższa o 27%** i utrzymywała się poniżej średniej z poprzednich 12 miesięcy. Jednocześnie w stosunku do sierpnia 2026 r. liczba incydentów **wzrosła o 2%.**

Liczba nazw szkodliwych domen wpisanych na Listę Ostrzeżeń CERT Polska I–IX 2026



CERT Polska prowadzi Listę Ostrzeżeń przed niebezpiecznymi stronami

Lista Ostrzeżeń służy do blokowania dostępu do szkodliwych stron internetowych. CERT Polska wykrywa podejrzane domeny dzięki swoim systemom oraz zgłoszeniom od użytkowników, dlatego każda informacja przyczynia się do zwiększenia bezpieczeństwa w sieci.

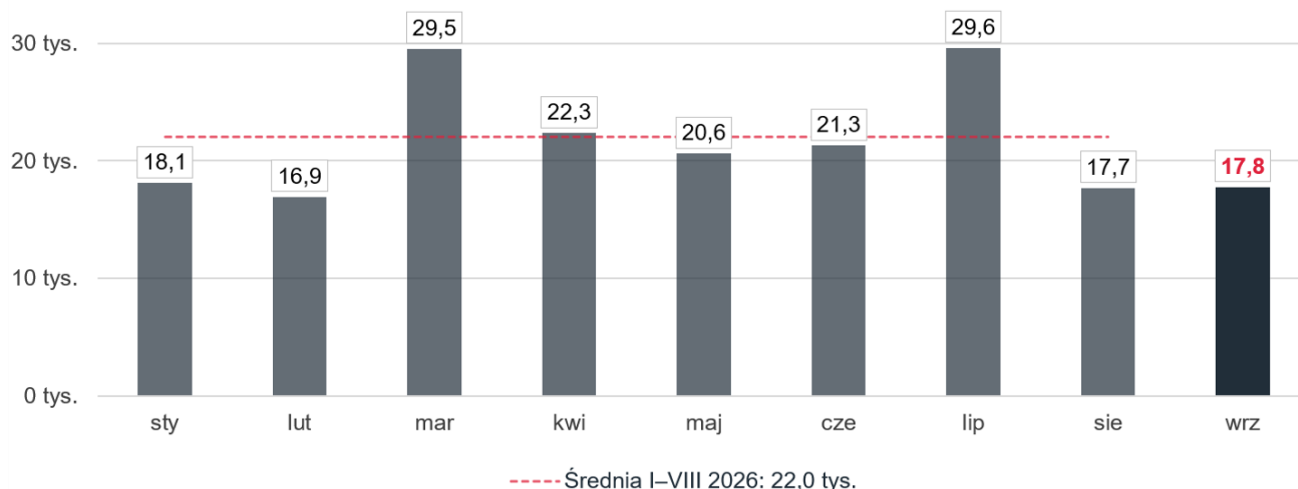
Podjętą stronę internetową, wiadomość e-mail zgłoś na
incydent.cert.pl
lub w usłudze
Bezpiecznie w sieci
w aplikacji mObywatel

Podjętą SMS prześlij pod numer
8080

CERT.PL
NASK

Na Listę Ostrzeżeń wpisywane są domeny, które wprowadzają użytkowników w błąd i wyłudniają od nich dane. Takie domeny są blokowane na okres **6 miesięcy**. Po upływie tego czasu, jeśli nadal zawierają niebezpieczne treści, zostają **ponownie wpisane na listę** jako nowy wpis.

Lista Ostrzeżeń jest wykorzystywana przez operatorów telekomunikacyjnych, firmy, organizacje i samych użytkowników do **automatycznego blokowania dostępu do szkodliwych stron internetowych**, co pozwala ograniczać skutki ataków phishingowych i innych kampanii wymierzonych w obywateli Polski.



Wykres 3. Liczba nazw szkodliwych domen wpisanych na Listę Ostrzeżeń. Źródło: CERT Polska / CSIRT NASK.

Od 1 stycznia do 30 września 2026 r. na Listę Ostrzeżeń przed niebezpiecznymi stronami wpisano **193,8 tys.** szkodliwych domen, z czego we wrześniu 2026 r. dodano **17,8 tys.** nazw domen wykorzystywanych do wyludzania danych osobowych, danych uwierzytelniających do kont bankowych i serwisów społecznościowych. Wartość ta w stosunku do sierpnia 2026 r. utrzymywała się na zbliżonym poziomie.

PRZYKŁADY NAZW FAŁSZYWYCH DOMEN



aldi.vsale.shop
allegrolokalnie.pl02.top
biedronka-food.shop
dhl-pl.top
govcpl.cfd
inpost.przelew-pl.shop
investui.net

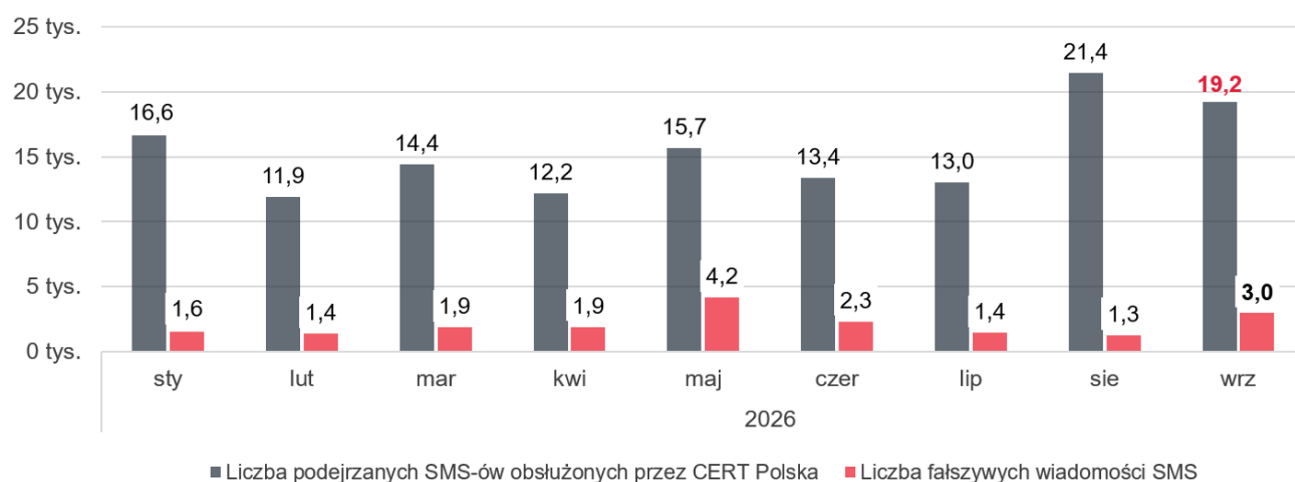
kapitalpolskaai.com
knfgovpl.site
olx.zakupy-24.sbs
pknorlen.shop
plmodalidl.shop
travelo-booking.com
vinted.finddin.com

Lista Ostrzeżeń zawierająca wykaz domen stanowiących zagrożenie znajduje się na stronie cert.pl/lista-ostrzezen



Liczba zgłoszeń wiadomości SMS przyjętych przez CERT Polska I–IX 2026

Od 1 stycznia do 30 września 2026 r. zespół CERT Polska zarejestrował **137,8 tys.** zgłoszeń podejrzanych SMS-ów. Liczba SMS-ów otrzymanych we wrześniu 2026 r. wyniosła **19,2 tys.** W porównaniu z sierpniem 2026 r. był to **spadek o 10%**. Wśród ogółu SMS-ów przyjętych we wrześniu 2026 r. **falszywe wiadomości**, czyli takie, w których nadawca podszywa się pod inny podmiot, aby skłonić odbiorcę wiadomości do określonego działania – np. podania danych osobowych, przekazania pieniędzy, wejścia na stronę internetową lub instalacji oprogramowania, **stanowiły 15%.**



Wykres 4. Liczba SMS-ów zgłoszonych do CSIRT NASK w danym miesiącu.

Wzorce falszyszych wiadomości SMS I–IX 2026

Zgodnie z ustawą z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej CSIRT NASK **monitoruje występowanie smishingu i tworzy wzorce wiadomości**, które posiadają cechy pozwalające na uznanie ich za smishing. Działania te wykonuje na podstawie zgłoszeń podejrzanych wiadomości tekstowych (SMS) otrzymanych od odbiorców tych wiadomości oraz informacji otrzymanych od przedsiębiorców telekomunikacyjnych i innych podmiotów, np. banków, firm kurierskich, platform inwestycyjnych. CSIRT NASK zapewnia dostęp do informacji o występowaniu smishingu wraz ze wzorcami wiadomości Komendantowi Centralnego Biura Zwalczania Cyberprzestępczości, Prezesowi Urzędu Komunikacji Elektronicznej i przedsiębiorcom telekomunikacyjnym. Podejrzane SMS-y można zgłaszać do CSIRT NASK poprzez bezpłatny skrócony numer **8080**. We wrześniu 2026 r., na podstawie wytworzonych przez CERT Polska wzorców falszyszych wiadomości SMS, zablokowano łącznie **28,0 tys.** SMS-ów. Dane o zablokowanych wiadomościach SMS są szacowane na podstawie raportów przesyłanych przez operatorów telekomunikacyjnych z uwzględnieniem procentowego udziału tych operatorów w rynku telefonii mobilnej.

Tabela 2. Liczba wytworzonych wzorców fałszywych wiadomości SMS.

Wzorce fałszywych wiadomości SMS w 2026	sty	lut	mar	kwi	maj	cze	lip	sie	wrz	Razem
Liczba wytworzonych wzorców	118	97	85	80	105	36	57	94	67	739

Wykaz wzorców wiadomości SMS znajduje się na stronie: telegraf.cert.pl

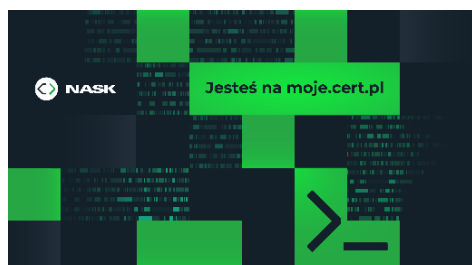
Moje.cert.pl

W 2025 r. zespół CERT Polska udostępnił bezpłatny serwis moje.cert.pl. Mogą z niego korzystać zarówno osoby prywatne posiadające stronę internetową, jak i firmy oraz instytucje publiczne. Zarejestrowany użytkownik moje.cert.pl może zamówić bezpłatne skanowanie bezpieczeństwa swoich domen, otrzymać informacje o wyciekach haseł użytkowników w swojej domenie, infekcjach szkodliwym oprogramowaniem i innych zagrożeniach w swoich sieciach (ta funkcja jest dostępna dla administratorów serwerów i sieci), a także sprawdzić, czy dana sieć jest chroniona przez Listę Ostrzeżeń przed niebezpiecznymi stronami.

W serwisie dostępne są także moduły: „**Infrastruktura organizacji**” (pozwala zobaczyć całość infrastruktury widocznej z internetu, np. subdomeny, hosty, otwarte porty i powiązane z nimi podatności) oraz „**Podatności w używanych technologiach**” (podmioty wyrażają zgodę na wykorzystanie informacji o swojej infrastrukturze, dzięki czemu system może je zestawiać ze zbieranymi na bieżąco informacjami o nowych lukach bezpieczeństwa, np. w bramkach VPN).

Ponadto w serwisie, w zakładce „Komunikaty” zespół CERT Polska publikuje ostrzeżenia dotyczące polskiej cyberprzestrzeni oraz alerty o podatnościach. Komunikaty te są dostępne na stronie także dla niezarejestrowanych użytkowników, można również otrzymywać je w wiadomości e-mail. [Moje.cert.pl](https://moje.cert.pl) korzysta m.in. z systemów **Artemis** (skanowanie stron) i **n6** (informacje o zagrożeniach dla adresacji IP) – narzędzi pozwalających chronić dane i infrastrukturę.

We wrześniu 2026 r. w serwisie moje.cert.pl **zarejestrowało się 1,4 tys. nowych użytkowników**.



W okresie od 1 do 30 września 2026 r. CERT Polska wysłał **15,9 tys. powiadomień w ramach serwisu moje.cert.pl dotyczących wykrytych podatności lub błędnych konfiguracji**. Powiadomienia o wykrytych nieprawidłowościach zostały wysłane do osób, które zgłosiły daną stronę do skanowania w serwisie moje.cert.pl, a także do ich współpracowników dodanych w serwisie.

Więcej: moje.cert.pl

Podatności CVE

Zespół CERT Polska od sierpnia 2023 r. pełni funkcję CNA (ang. *CVE Numbering Authority*) – współtworzy bazę podatności poprzez nadawanie numerów CVE, które służą do identyfikacji i katalogowania publicznie ujawnionych podatności (więcej: [CERT Polska/CNA](#)). We wrześniu 2026 r. zespół CERT Polska nadał **35** numerów CVE. Wśród wykrytych podatności znalazły się podatności w oprogramowaniu m.in. drEryk Gabinet, WEBCON BPS, w module „raty” Alior Bank dla PrestaShop, Dayforce Payroll, Das U-Boot, Ghostscript, Quick.Cart. W ramach badań własnych CERT Polska znalazł 13 podatności: w oprogramowaniu MikroTik RouterOS (6 podatności) i urządzeniach F&F Filipowski mH-DEVELOPER (7 podatności).

Lista opublikowanych podatności dostępna jest na stronie: [CERT Polska/CVE](#)

Tabela 3. Nadane numery CVE od 1 stycznia do 30 września 2026 r.

Numery CVE w 2026	sty	lut	mar	kwi	maj	cze	lip	sie	wrz	Razem
Liczba opublikowanych numerów CVE	16	12	32	21	34	47	53	33	35	283

Wybrane podatności i ich wpływ na krajobraz cyberbezpieczeństwa w Polsce – IX 2026

**CVE-2026-67276 (CVSS 9.2), CVE-2026-67277 (CVSS 8.8),
CVE-2026-67278 (CVSS 6.3), CVE-2026-67279 (CVSS 6.9),
CVE-2026-67281 (CVSS 8.7), CVE-2026-86060 (CVSS 9.2)**

**Aktywnie wykorzystywane podatności
w MikroTik RouterOS**

12 309

Liczba podatnych instancji

677

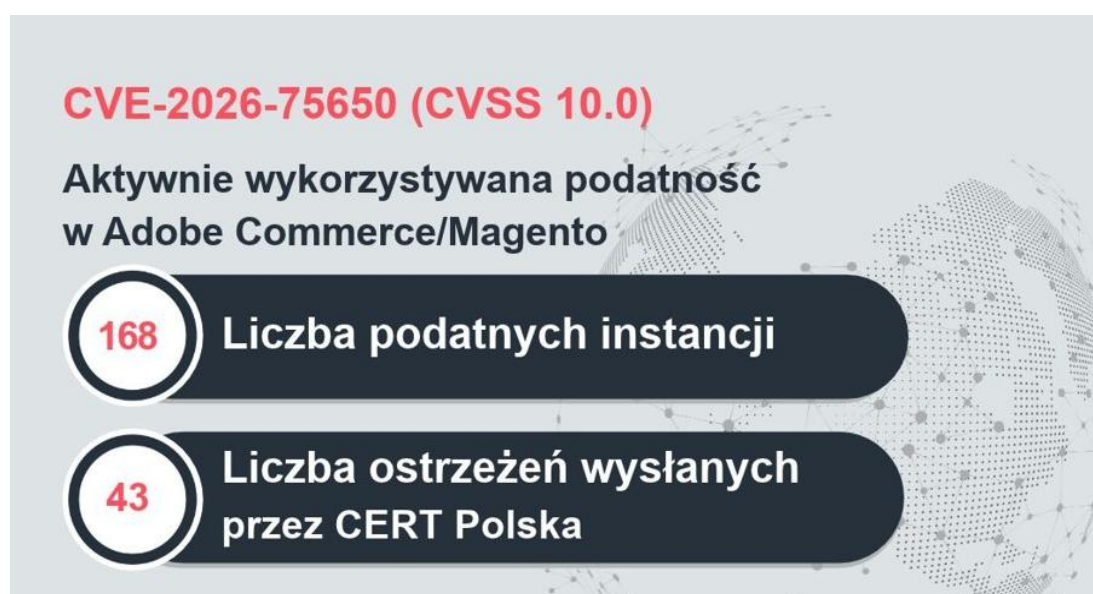
**Liczba ostrzeżeń wysłanych
przez CERT Polska**

Zestawienie podatności, w tym dwóch krytycznych, w systemie RouterOS urządzeń MikroTik. Zostały one odkryte przez zespół CERT Polska w badaniach własnych, zespół koordynował też proces ich ujawniania (CVD). Podatność oznaczona jako CVE-2026-67276 pozwala obejść uwierzytelnianie SSH bez klucza prywatnego. RouterOS sprawdza typ klucza i moduł klucza RSA,

ale pomija wykładnik, co pozwala sfabrykować poprawny podpis i przejąć urządzenie. Pozostałe CVE obejmują m.in. uwierzytelnianie bez logowania w SSH i WebFig oraz wstrzykiwanie argumentów w ścieżce logowania.

Rekomendujemy: aktualizację oprogramowania do wersji RouterOS 6.49.21, 7.23.4 (lub 7.23.6), 7.24.2 (lub 7.24.3), wyłączenie dostępu SSH/WebFig z internetu i audyt kluczy.

Więcej: <https://cert.pl/posts/2026/09/mikrotik-routeros-cve>, <https://cert.pl/posts/2026/09/podatnosci-w-mikrotik-routeros-aktywnie-wykorzystywane>, <https://mikrotik.com/supportsec/september-2026-vulnerability>



Krytyczna podatność w platformie sklepowej Adobe Commerce pozwalająca na zdalne wykonanie kodu bez logowania i bez interakcji użytkownika. Luka jest aktywnie wykorzystywana w atakach z użyciem narzędzia StyleSmuggler i figuruje w wykazie CISA KEV. Możliwe skutki obejmują przejęcie sklepu i kradzież danych klientów.

Rekomendujemy: instalację poprawki APSB26-146, ograniczenie dostępu do panelu administracyjnego i audyt serwera.

Więcej: <https://helpx.adobe.com/security/products/magento/apsb26-146.html>, https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-75650

CVE-2026-63219 (CVSS 8.6),**CVE-2026-58400 (CVSS 9.1)****Aktywnie wykorzystywane podatności
w GeoNetwork****8****Liczba podatnych instancji****10****Liczba ostrzeżeń wysłanych
przez CERT Polska**

Krytyczne podatności w aplikacji GeoNetwork, umożliwiające zdalne wykonanie kodu bez logowania. Atakujący przez przeglądarkę może przejąć serwer, ukraść dane i poświadczenia. Instancje powinny zostać zaktualizowane, a dostęp do nich ograniczony.

Rekomendujemy: aktualizację do najnowszej wersji, ograniczenie dostępu sieciowego i audyt logów.

Więcej: <https://nvd.nist.gov/vuln/detail/CVE-2026-63219>, <https://nvd.nist.gov/vuln/detail/CVE-2026-58400>

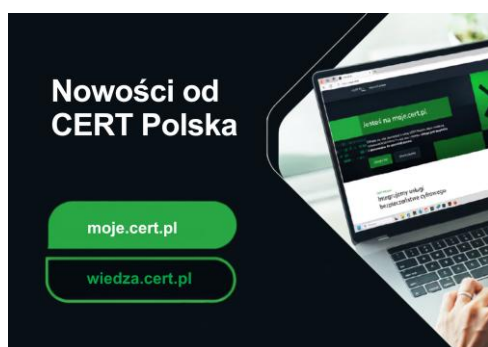
CVE-2026-85102 (CVSS 9.8),**CVE-2026-85103 (CVSS 9.8)****Aktywnie wykorzystywane podatności
w Check Point Quantum Security Gateway****3 056****Liczba podatnych instancji****281****Liczba ostrzeżeń wysłanych
przez CERT Polska**

Krytyczne podatności w firewallu Check Point pozwalające na zdalne wykonanie kodu podczas negocjacji VPN bez konieczności logowania. Luka jest aktywnie wykorzystywana i znajduje się w katalogu CISA KEV. Możliwe skutki obejmują przejęcie urządzenia i kradzież konfiguracji VPN.

Rekomendujemy: instalację poprawki SK (sk1000117), wyłączenie dostępu do zarządzania z internetu i analizę logów VPN.

Więcej: <https://support.checkpoint.com/results/sk/sk1000117>,
<https://blog.checkpoint.com/security/security-advisory-action-required-active-exploitation-of-cve-2026-85102-and-a-management-pre-authentication-vulnerability-cve-2026-93616>,
https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-85102,
<https://nvd.nist.gov/vuln/detail/cve-2026-85103>

Wybrane informacje



2 września **zespół CERT Polska** uruchomił ogólnodostępny portal wiedza.cert.pl. Jego celem jest wspieranie użytkowników indywidualnych, administratorów IT oraz osoby odpowiedzialne za ochronę infrastruktury instytucji publicznych i prywatnych w budowaniu i rozwijaniu kompetencji w zakresie cyberbezpieczeństwa. Składa się z sekcji: „Ścieżki postępowania” (scenariusze działań w przypadku np. phishingu czy ransomware), „Obsługa incydentów” (procedury reagowania na incydenty bezpieczeństwa – krok po kroku), „Bezpieczeństwo osobiste” (porady i wskazówki dla użytkowników indywidualnych), „Dobre praktyki” (zbiór rekomendacji), „Odporność infrastruktury” (materiały m.in. na temat bezpieczeństwa środowisk przemysłowych), „Polityki i procedury” (m.in. wzory dokumentacji, obowiązujące regulacje prawne), „Systemy CERT Polska” (informacje o systemach i usługach wspierających monitorowanie i ochronę infrastruktury).

Ponadto zespół CERT Polska udostępnił w serwisie moje.cert.pl nową funkcjonalność dla zarejestrowanych użytkowników – „Podatności w używanych technologiach”, dzięki której podmioty mogą otrzymywać informacje o nowych lukach bezpieczeństwa w ich infrastrukturze, np. w bramkach VPN czy w systemach zarządzania treścią.

Więcej: [cert.pl/Nowości od CERT Polska – premiera wiedza.cert.pl i nowa funkcja w moje.cert.pl](https://cert.pl/Nowości%20od%20CERT%20Polska%20-%20premiera%20wiedza.cert.pl%20i%20nowa%20funkcja%20w%20moje.cert.pl)



5 września zespół CERT Polska opublikował artykuł pt. „**Krytyczne podatności w MikroTik RouterOS są aktywnie wykorzystywane. Zalecana pilna aktualizacja**”. Są to podatności, które zespół zidentyfikował oraz których ujawnienie koordynował. Zostały one odnalezione przy użyciu modeli GPT-5.5-cyber i GPT-5.6-sol w ramach dostępu do programu OpenAI Government and Trust Agency Collaboration GTAC. 22 września ukazał się artykuł uzupełniający analizę pt. „**MikroTrick: analiza techniczna, proces ujawnienia i zastosowanie agentów LLM**”.

Więcej: [cert.pl/Krytyczne podatności w MikroTik RouterOS są aktywnie wykorzystywane. Zalecana pilna aktualizacja](https://cert.pl/Krytyczne_podatności_w_MikroTik_RouterOS_są_aktywnie_wykorzystywane._Zalecana_pilna_aktualizacja), [cert.pl/MikroTrick: analiza techniczna, proces ujawnienia i zastosowanie agentów LLM](https://cert.pl/MikroTrick:_analiza_tekniczna,_proces_ujawnienia_i_zastosowanie_agentów_LLM)



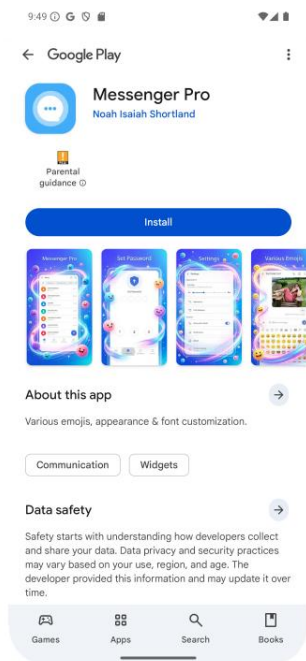
11 września **zaczął obowiązywać art. 14 aktu o cyberodporności (Cyber Resilience Act, CRA)**, na podstawie którego producenci oprogramowania i produktów z elementami cyfrowymi są zobowiązani do zgłaszania aktywnie wykorzystywanych podatności oraz poważnych incydentów mających wpływ na bezpieczeństwo ich produktów. Służy do tego pojedyncza platforma sprawozdawcza (Single Reporting Platform, SRP), zarządzana przez ENISA. SRP jest centralnym punktem zgłaszania incydentów i podatności w całej UE. Jest też przeznaczona dla polskich producentów, a ich **zgłoszenia są obsługiwane przez CSIRT NASK, który pełni funkcję koordynatora procesu ujawniania podatności**.

Więcej: [gov.pl/Europejska platforma zgłaszania podatności i incydentów w ramach aktu o cyberodporności](https://gov.pl/Europejska_platforma_zgłaszania_podatności_i_incydentów_w_ramach_aktu_o_cyberodporności), [cert.pl/CRA – nowe obowiązki dla producentów oprogramowania i korzyści dla użytkowników](https://cert.pl/CRA_-_nowe_obowiązki_dla_producentów_oprogramowania_i_korzyści_dla_użytkowników)



W ramach Centrum Cyberbezpieczeństwa NASK (CCN) powstaje **Krajowe Centrum Odzyskiwania Danych (KCOD)**, którego głównym zadaniem będzie wspieranie procesu reagowania na incydenty poprzez odzyskiwanie danych, ich analizę, a także pomoc zaatakowanym podmiotom w przywracaniu ciągłości działania po cyberatakach. Ponadto w KCOD eksperci będą analizować cyfrowe ślady w postaci danych, które zostawili po sobie atakujący.

Więcej: [nask.pl/Co po cyberataku? Nowe Centrum powstaje w NASK](https://nask.pl/Co_po_cyberataku?Nowe_Centrum_powstaje_w_NASK)



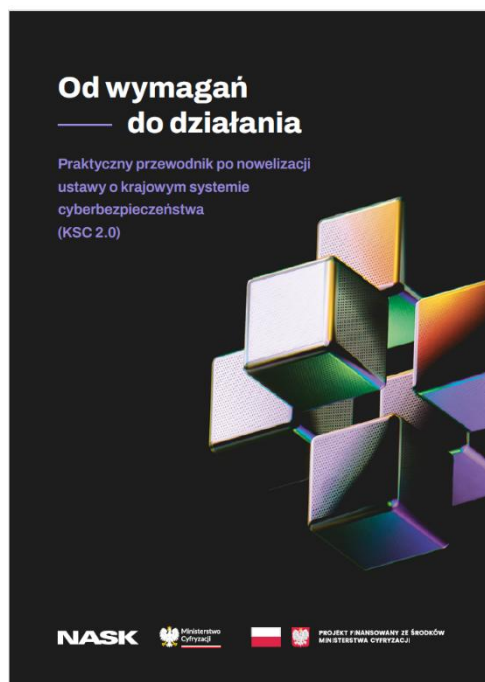
23 września na stronie cert.pl ukazało się opracowanie pt. **„Fałszywe reklamy i złośliwe aplikacje – analiza operacji toll fraud”**, podsumowujące badania przeprowadzone przez zespół CERT Polska. Punktem wyjścia były dwie reklamy na Facebooku, które ostrzegały polskich użytkowników, że ich aplikacja do obsługi plików PDF straciła ważność. Obie reklamy prowadziły jednak do Messenger Pro w Google Play, komunikatora niezwiązanego z plikami PDF. Po instalacji aplikacja uruchamiała czterowarstwowy łańcuch prowadzący do modułu realizującego toll fraud, który polega na nadużyciu mechanizmów płatności mobilnych w celu uruchomienia płatnej usługi bez wiedzy i świadomej zgody abonenta. We wrześniu zespół zgromadził dowody, które łączą 17 aplikacji z Google Play oraz 852 reklamy w Meta ze skoordynowaną operacją wymierzoną w polskich użytkowników Androida. Trwa monitorowanie dalszego rozwoju tej kampanii, a o kolejnych ustaleniach będziemy informować w następnych raportach.

Więcej: [cert.pl/Falszywe reklamy i złośliwe aplikacje – analiza operacji toll fraud](https://cert.pl/Falszywe_reklamy_i_zlosliwe_aplikacje_-_analiza_operacji_toll_fraud)



30 września – 1 października w Pałacu Kultury i Nauki w Warszawie odbyło się **VIII Forum Cyberbezpieczeństwa**, zorganizowane przez Ministerstwo Cyfryzacji. Wydarzenie zgromadziło przedstawicieli administracji, sektora prywatnego oraz ekspertów, w tym także z NASK – PIB, którzy rozmawiali o najważniejszych wyzwaniach cyfrowej rzeczywistości. Tematy, takie jak współczesne cyberzagrożenia i wyzwania z nimi związane, cyberodporność, reagowanie na incydenty, walka z dezinformacją, regulacje prawne, polityki bezpieczeństwa, rozpatrywano zarówno w ujęciu krajowym, jak i międzynarodowym w gronie zaproszonych gości reprezentujących europejskie i światowe instytucje. Współpracy międzynarodowej CSIRT-ów poświęcony był panel, prowadzony przez dyrektora Pionu CSIRT NASK, a kierownik CERT Polska wystąpił z prezentacją na temat reagowania na incydenty. W trakcie wydarzenia oficjalnie otwarto tegoroczny Europejski Miesiąc Cyberbezpieczeństwa.

Więcej: [nask.pl/Cyberodporność – nasza wspólna tarcza. NASK na Forum Cyberbezpieczeństwa](https://nask.pl/Cyberodporność_-_nasza_wspólna_tarcza_NASK_na_Forum_Cyberbezpieczeństwa)



NASK – PIB we współpracy z Ministerstwem Cyfryzacji przygotował poradnik pt. „**Od wymagań do działania. Praktyczny przewodnik po nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa (KSC 2.0)**”. Jego celem jest wsparcie organizacji w zrozumieniu i realizacji wymagań, które nakłada na nie nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa. Autorzy publikacji wyjaśniają proces samoidentyfikacji podmiotu, obowiązki ustawowe z perspektywy zarządzania, procedur, zabezpieczeń technicznych i codziennej pracy, a także kwestie dotyczące odpowiedzialności, kontroli i sankcji. Ponadto w poradniku znajdują się słowniczek najważniejszych pojęć oraz zestawienie źródeł na temat aktów prawnych i ich interpretacji, a także odnośniki do materiałów edukacyjnych, eksperckich oraz do narzędzi i standardów.

Więcej: [nask.pl/KSC 2.0 krok po kroku. Nowy poradnik NASK dla firm i instytucji](https://nask.pl/KSC_2.0_krok_po_kroku._Nowy_poradnik_NASK_dla_firm_i_instytucji)

Wystąpienia ekspertów CERT Polska

- 8–10 września – prowadzenie szkolenia dla administratorów na temat reagowania na incydenty, Czarnogóra.
Więcej: [wb3c.org/We just got hacked/relacja](https://wb3c.org/We_just_got_hacked/relacja)
- 11 września – prezentacja poświęcona najpoważniejszym cyberzagrożeniom („Polish Internet Threat Landscape”) na spotkaniu French Security & Defense Days Poland w Ambasadzie Francji, Warszawa.
Więcej: b2match.com/informacje
- 17 września – prezentacja pt. „ArtePhish: Interpretable Phishing Campaign Identification via Automated Artifact Discovery” na temat prowadzonych badań, SECAI – wydarzenie towarzyszące 31st European Symposium on Research in Computer Security (ESORICS) 2026, Rzym.
Więcej: [sites.google.com/SECAI 2026/informacje i program](https://sites.google.com/SECAI_2026/informacje_i_program)
- 17 września – prowadzenie warsztatów „Krajobraz cyberbezpieczeństwa – praktyczne porady dla JST” podczas Smart City Expo Poland w Warszawie.
Więcej: [smartcityexpo.pl/informacje i program](https://smartcityexpo.pl/informacje_i_program)
- 17 września – prezentacja „Największe cyberzagrożenia dla Polski i sektora akademickiego w 2026 roku” na Podkarpackim Forum Bezpieczeństwa, Uniwersytet Rzeszowski.
Więcej: [ur.edu.pl/informacje i program](https://ur.edu.pl/informacje_i_program)

- 26 września ukazała się rozmowa z kierownikiem CERT Polska. Jej tematem były najczęstsze błędy popełniane przez organizacje odnośnie do zabezpieczeń infrastruktury oraz najważniejsze zasady, których stosowanie pomaga zminimalizować ryzyko ataku.

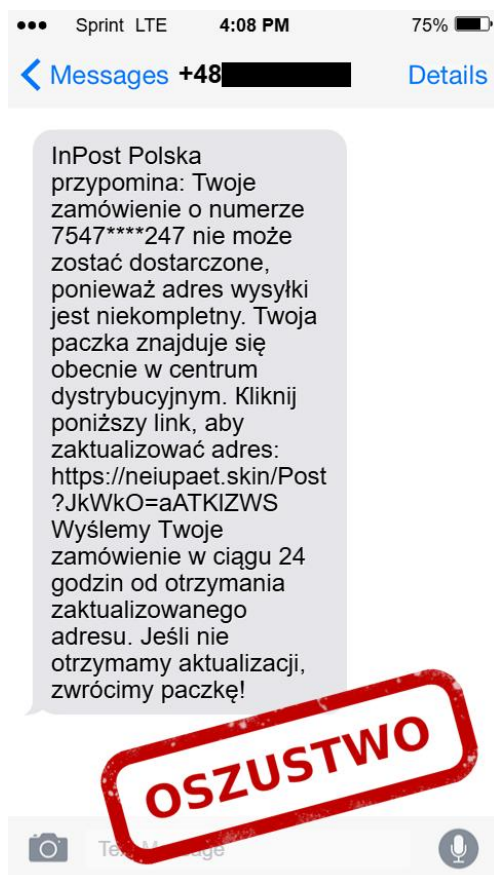
Więcej: [cyberdefence24.pl/Szef CERT Polska o cyberbezpieczeństwie. „90% zaszyfrowanych backupów”](https://cyberdefence24.pl/Szef-CERT-Polska-o-cyberbezpiecztwie-90-zaszyfrowanych-backupow)

- 29 i 30 września podczas 78. Spotkania TF-CSIRT w Sztokholmie eksperci przedstawili prezentacje dotyczące nowych funkcjonalności w serwisie moje.cert.pl („Free security tools for everyone in Poland: an update”) oraz na temat doświadczeń zespołu CERT Polska w koordynowaniu ujawniania podatności („National CSIRT as a CVD Hub: Lessons from CERT.PL’s Vulnerability Coordination Cases”).

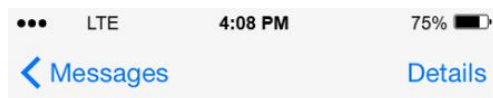
Więcej: [tf-csirt.org/78th TF-CSIRT Meeting/informacje i program](https://tf-csirt.org/78th-TF-CSIRT-Meeting/informacje-i-program)

Komunikaty o zagrożeniach

Informacje o zaobserwowanych kampaniach publikowane przez zespół CERT Polska w serwisie moje.cert.pl oraz w serwisach społecznościowych.



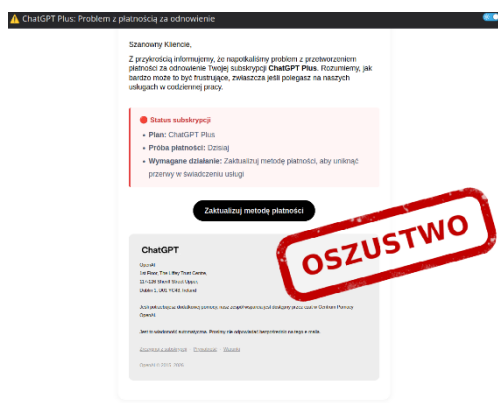
Zespół CERT Polska obserwował kampanię phishingową, w której cyberprzestępcy podszywają się pod firmy kurierskie. Oszuści wysyłają SMS-y z informacją o rzekomych problemach z doręczeniem przesyłki oraz podają link prowadzący do formularza, za pomocą którego próbują wyłudzić dane osobowe użytkownika.



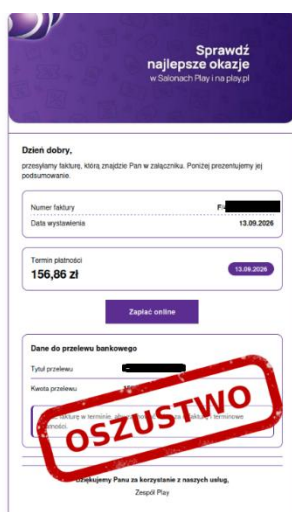
Zespół CERT Polska monitorował kampanię phishingową, w której oszuści podszywają się pod administrację publiczną. W wiadomościach SMS umieszczają informację o rzekomej konieczności aktualizacji danych oraz link prowadzący do strony phishingowej. Szata graficzna fałszywej strony jest łudząco podobna do oficjalnego serwisu rządowego w domenie gov.pl. Pod pretekstem logowania do serwisu przestępcy kierują użytkownika najpierw do fałszywego formularza logowania do bankowości elektronicznej, a następnie do formularza służącego do wyłudzenia danych osobowych oraz adresowych.



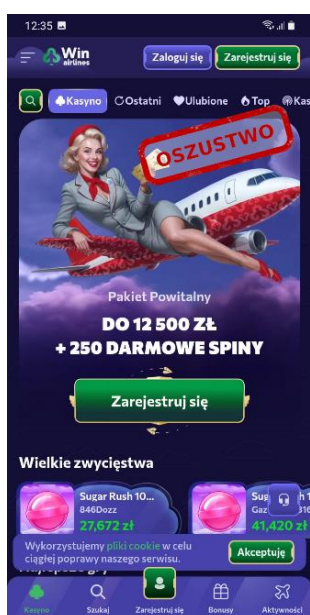
Zespół CERT Polska monitorował kolejną kampanię SMS-ową, w której oszuści podszywają się pod rządowy serwis e-TOLL. W wysyłanych wiadomościach informują o rzekomym wykroczeniu drogowym i zachęcają do sprawdzenia informacji na ten temat na stronie, do której prowadzi podany przez nich link. Jest to strona wykorzystująca wizerunek serwisu e-TOLL, gdzie podana jest kwota do uregulowania za wykroczenie. W następnym kroku użytkownik jest proszony o podanie danych karty płatniczej oraz numeru rejestracyjnego pojazdu. Dane trafiają do oszustów.



Zespół CERT Polska informował o kampanii phishingowej, w której oszuści wykorzystują wizerunek firmy OpenAI. Wysyłają e-maile o rzekomych trudnościach z przetworzeniem płatności za odnowienie subskrypcji ChatGPT Plus. W wiadomości znajduje się odnośnik z napisem „Zaktualizuj metodę płatności”, który prowadzi na stronę zawierającą formularz, za pomocą którego oszuści próbują wyłudzić dane karty płatniczej.



Zespół CERT Polska obserwował kampanię phishingową skierowaną do klientów operatora sieci komórkowej Play. Oszuści wysyłają wiadomości e-mail, w których informują o rzekomej konieczności opłacenia faktury. W wiadomości znajduje się odnośnik prowadzący na stronę imitującą witrynę operatora, gdzie znajduje się formularz płatności służący do wyłudzenia danych osobowych oraz danych karty płatniczej.



Zespół CERT Polska obserwował nowy sposób działania oszustów. Cyberprzestępcy wykorzystują mechanizmy reklamowe smartfonów do wyświetlania powiadomień przypominających komunikaty od znanych aplikacji, takich jak sklepy, programy lojalnościowe czy platformy zakupowe. Na ekranie smartfona pojawia się powiadomienie wykorzystujące nazwę lub logo popularnej usługi, ale po kliknięciu zamiast do aplikacji użytkownik jest przenoszony na zewnętrzną stronę internetową. Może ona służyć m.in. do promowania niechcianych usług lub wyłudzenia danych. Problem dotyczył smartfonów Xiaomi, Oppo oraz Realme, ale podatne mogą być także inne marki oferujące wyświetlanie zewnętrznych reklam w systemie operacyjnym telefonu.



Zespół CERT Polska odnotował wzrost liczby reklam w mediach społecznościowych, głównie na Facebooku, które prowadzą do stron podszywających się pod znany sklep z odzieżą i akcesoriami wojskowymi. Reklamy te, publikowane z różnych kont, zachęcają do skorzystania z atrakcyjnych promocji. Celem oszustów może być pozyskanie danych osobowych, danych potrzebnych do realizacji płatności lub pieniędzy za zamówienie, które w rzeczywistości nie zostanie zrealizowane.



Zespół CERT Polska obserwował kampanię reklamową w mediach społecznościowych, w której oszuści informują o rzekomych rabatach na paliwo. W reklamach wykorzystywany jest wizerunek znanych marek, m.in. Orlenu, oraz różnych banków. Przekaz sugeruje możliwość uzyskania zniżek na tankowanie, myjnię, zakupy na stacji. Link z reklamy prowadzi do strony internetowej przygotowanej przez oszustów. Ich celem jest pozyskanie danych – numeru telefonu i danych karty płatniczej. W efekcie zamiast obiecanego rabatu można stracić pieniądze lub narazić się na dalsze próby oszustwa.

Więcej: [Facebook/CERT Polska](https://www.facebook.com/CERTPolska), [X/CERT Polska](https://twitter.com/CERTPolska), moje.cert.pl/komunikaty, [LinkedIn/CERT Polska](https://www.linkedin.com/company/CERTPolska)

Podejrzane SMS-y i e-maile

Nie spiesz się. Presja czasu wywierana w wiadomości to znak ostrzegawczy

Zwracaj uwagę na rozszerzenia plików załączonych do wiadomości. Formaty takie jak .rar, .zip, .exe, .js mogą sugerować, że zawartość załącznika jest inna niż opisana w treści e-maila

Jak się chronić?

Zweryfikuj adres nadawcy e-maila. W razie wątpliwości zadzwoń do instytucji, która rzekomo wysłała wiadomość

Stosuj mocne hasła i uwierzytelnienie dwuskładnikowe. Więcej informacji na ten temat znajdziesz na stronie cert.pl/bezpieczne-hasla

Pamiętaj: oferta inwestycji z obietnicą szybkiego zysku może być oszustwem

Po kliknięciu w link upewnij się, że jesteś na właściwej stronie – dokładnie sprawdź adres widoczny w pasku przeglądarki

CERT.PL > NASK

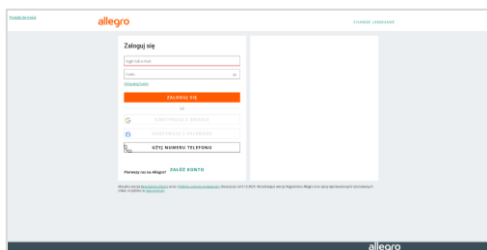
Opis najczęściej występujących kampanii – IX 2026

Fałszywe strony oferujące wysokodochodowe inwestycje



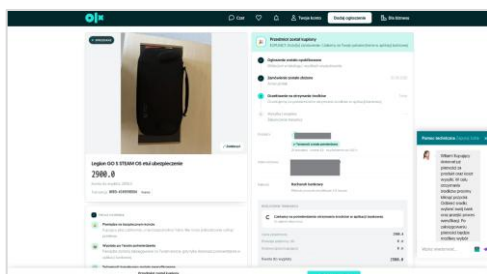
Zespół CERT Polska w dalszym ciągu obserwował wzmożoną kampanię phishingową, w której oszuści podszywają się pod różnego rodzaju koncerny paliwowo-energetyczne, firmy i instytucje, m.in. Lotos, Orlen, Tesla, PGNiG, PGE, Baltic Pipe. Oszuści reklamują w mediach społecznościowych oraz w serwisach internetowych nieistniejące programy dla akcjonariuszy indywidualnych, a także rozsyłają wiadomości, w których informują o możliwości inwestowania środków z rzekomo wysokim zyskiem za pośrednictwem platform inwestycyjnych. Osoby zainteresowane dużymi zarobkami oraz inwestycjami w handel ropą, gazem czy akcje firmy są proszone o udostępnienie swoich danych osobowych i kontaktowych w formularzu, do którego prowadzi link umieszczony w reklamie lub wiadomości. Następnie z użytkownikiem kontaktuje się telefonicznie osoba podająca się za konsultanta i zachęca do zainwestowania środków w kryptowaluty, obligacje czy akcje firm na platformie, która – jak się później okazuje – uniemożliwia wypłatę zainwestowanych pieniędzy. Celem oszustów jest wyłudzenie środków finansowych.

Fałszywe strony wykorzystujące wizerunek serwisu Allegro



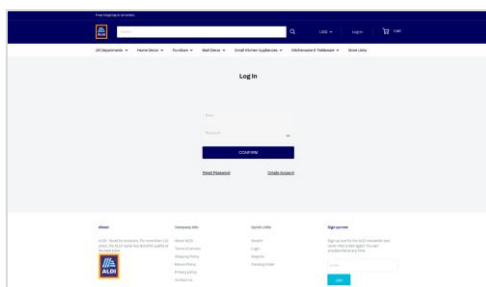
Zespół CERT Polska obserwował wzmożoną kampanię phishingową, w której oszuści wykorzystującą wizerunek platformy Allegro. Na fałszywych stronach internetowych znajduje się panel logowania do tego serwisu służący do wyłudzenia danych uwierzytelniających od użytkowników Allegro.

Fałszywe strony podszywające się pod serwis OLX



Zespół CERT Polska zarejestrował incydenty, w których atakujący za pośrednictwem stron internetowych podszywają się pod serwis OLX. Strony zawierają fałszywy panel logowania do serwisu lub fałszywy panel płatniczy. Celem oszustów jest wyłudzenie danych uwierzytelniających lub kradzież środków finansowych.

Fałszywe strony wykorzystujące markę ALDI



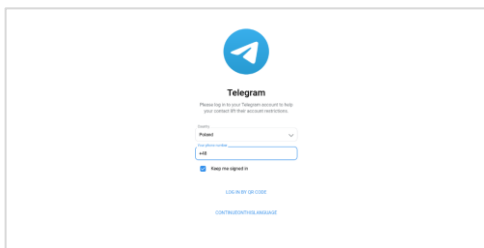
Zespół CERT Polska obserwował incydenty, w których oszuści tworzą fałszywe sklepy internetowe z wykorzystaniem wizerunku sieci sklepów ALDI. Celem oszustów jest wyłudzenie od użytkowników danych uwierzytelniających oraz kradzież środków finansowych.

Fałszywe strony serwisu Gazeta.pl



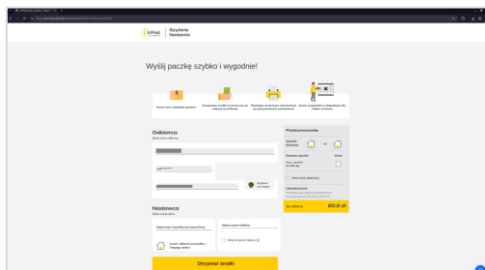
Zespół CERT Polska rejestrował incydenty, w których atakujący za pośrednictwem stron internetowych podszywają się pod serwis Gazeta.pl. Na spreparowanych stronach oszuści publikują artykuły, w których wykorzystują wizerunki znanych osób do promowania fałszywych platform inwestycyjnych.

Fałszywe strony podszywające się pod komunikator Telegram



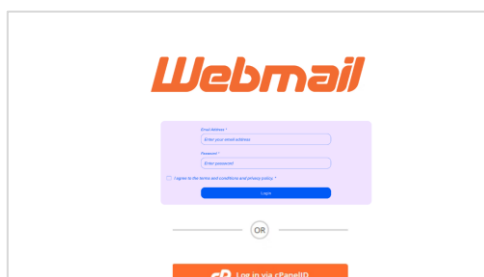
Zespół CERT Polska obserwował kampanię mającą na celu przejmowanie kont użytkowników komunikatora Telegram. Oszuści wysyłają wiadomości SMS z informacją, że konto użytkownika mogło brać udział w wysyłce spamu. Link zawarty w wiadomości prowadzi do strony internetowej, która wyłudza numer telefonu. Następnie użytkownik jest proszony o wpisanie kodu weryfikacyjnego wysłanego na jego numer – podanie go umożliwia atakującym przejęcie konta Telegram.

Fałszywe strony wykorzystujące wizerunek firmy InPost



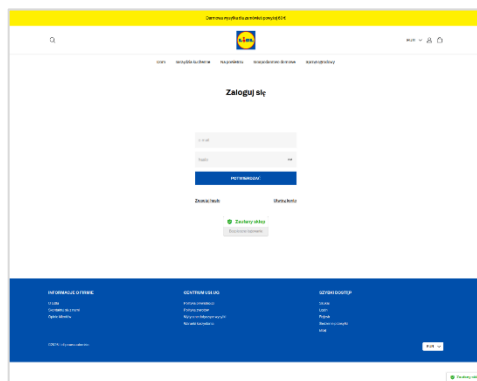
Zespół CERT Polska rejestrował incydenty, w których oszuści podszywają się pod firmę InPost. Celem są użytkownicy serwisu OLX lub Vinted. Oszuści kontaktują się z potencjalną ofiarą. Wyrażają zainteresowanie przedmiotem z ogłoszenia, następnie informują, że dokonali opłaty, i wysyłają link do strony internetowej, poprzez którą rzekomo można wypłacić środki. Witryna wykorzystuje wizerunek firmy InPost. Znajduje się na niej fałszywy panel płatniczy. Podanie danych karty powoduje utratę środków finansowych przechowywanych na koncie bankowym.

Fałszywe panele logowania do aplikacji typu webmail



Zespół CERT Polska rejestrował incydenty, w których oszuści tworzą fałszywe strony internetowe zawierające podrobiony panel logowania do aplikacji typu webmail, umożliwiającej dostęp do poczty elektronicznej za pośrednictwem przeglądarki internetowej. Celem oszustów jest pozyskanie danych logowania do poczty.

Fałszywe panele logowania wykorzystujące markę Lidl



Zespół CERT Polska obserwował incydenty, w których oszuści wykorzystują wizerunek marki Lidl. Na fałszywych stronach internetowych znajduje się panel logowania do sklepu internetowego. Celem oszustów jest pozyskanie od użytkowników danych uwierzytelniających.