SIERPIEŃ 2026

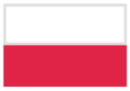
Podsumowanie Miesiąca CERT POLSKA

Nr 8/2026

CERT.PL NASK

CSIRT NASK

PODSUMOWANIE MIESIĄCA CERT POLSKA



PROJEKT FINANSOWANY ZE ŚRODKÓW MINISTERSTWA CYFRYZACJI

TLP: CLEAR

Autor: zespół CERT Polska

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 – VIII 2026 10

Wybrane informacje 13

Wystąpienia ekspertów CERT Polska 14

Komunikaty o zagrożeniach 14

Opis najczęściej występujących kampanii – VIII 2026 19

Statystyki zgłoszonych zagrożeń oraz zarejestrowanych incydentów

Zgłoszenia i incydenty cyberbezpieczeństwa

Statystyki przedstawione w tym rozdziale obejmują dane o liczbie zgłoszeń[1] oraz o liczbie incydentów obsłużonych przez CSIRT NASK w okresie od 1 do 31 sierpnia 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 – VIII 2026

Tabela 1. Liczba zgłoszeń oraz zarejestrowanych incydentów od 1 do 31 sierpnia 2026 r.

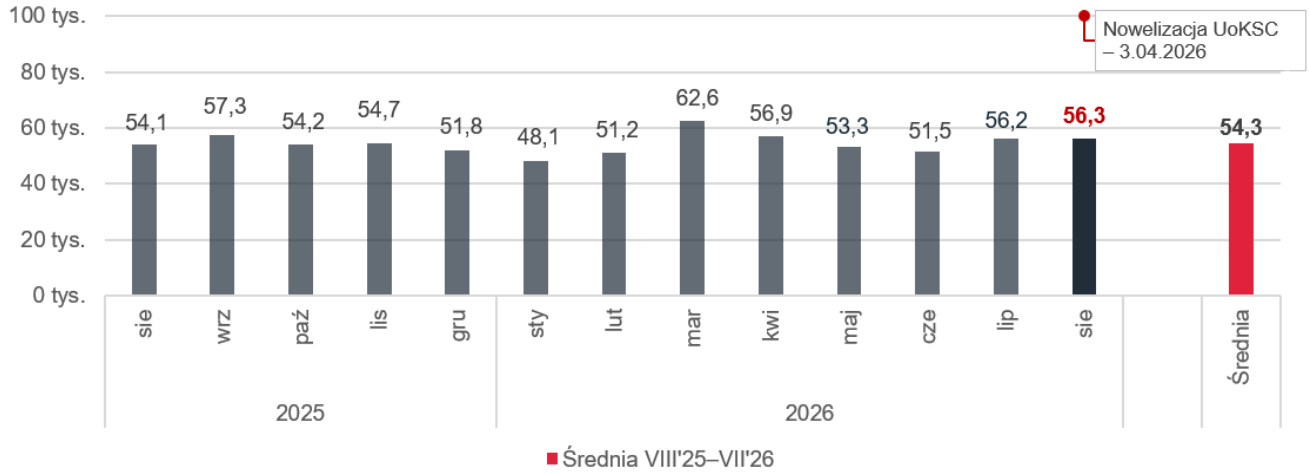
Zgłoszone zagrożenia i zarejestrowane incydenty	Liczba
Zgłoszenia potencjalnych zdarzeń dla cyberbezpieczeństwa*	4,7 tys.
Zgłoszenia cyberzagrożeń*	48,9 tys.
Zgłoszenia incydentów	2,7 tys.
Zgłoszenia poważnych cyberzagrożeń*	0,02 tys.
Razem zgłoszenia	**56,3 tys.**
Zarejestrowane incydenty**	**18,9 tys.**

* 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.

W sierpniu 2026 r. zespół CERT Polska otrzymał **łącznie 56,3 tys. zgłoszeń**. Na ich podstawie **zarejestrowano 18,9 tys. incydentów** cyberbezpieczeństwa, które miały lub mogły mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych. Dotyczą one konkretnych kategorii zagrożeń, np. szkodliwych stron wyłudzających poufne informacje (ang. *phishing*), spamu czy ataku z użyciem szkodliwego oprogramowania. W wielu przypadkach jeden incydent był powiązany z kilkoma zgłoszeniami.

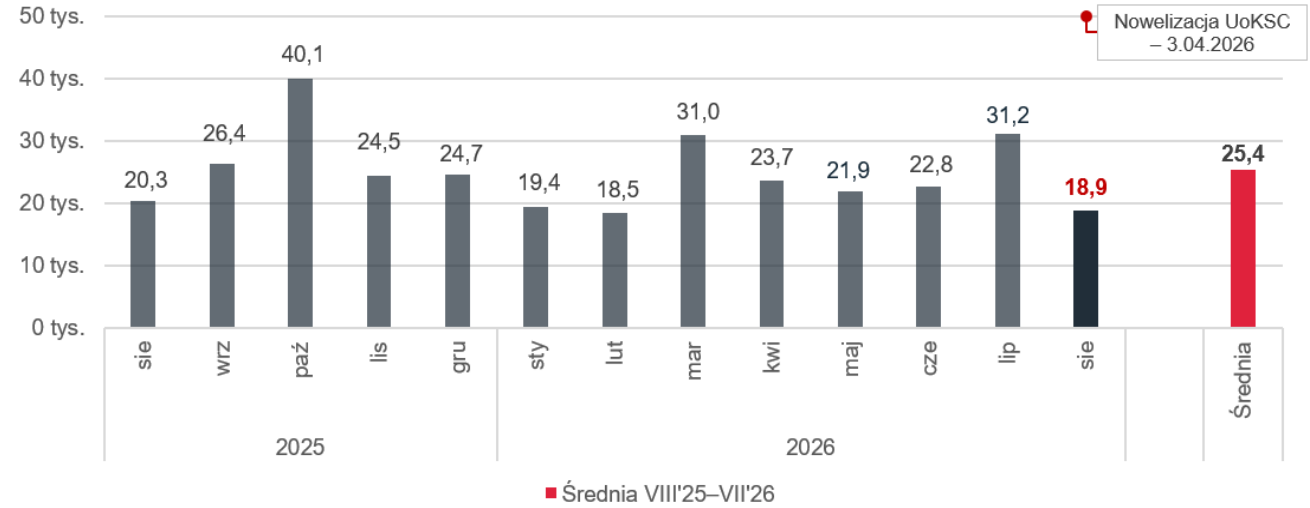
Zgłoszenia zagrożeń od VIII 2025 do VIII 2026



Wykres 1. Liczba wszystkich zgłoszeń od 01.08.2025 do 31.08.2026. Źródło: CERT Polska / CSIRT NASK.

Liczba wszystkich zgłoszeń odnotowanych w sierpniu 2026 r. pozostawała powyżej średniej liczonej z poprzednich 12 miesięcy. W porównaniu z analogicznym miesiącem 2025 r. liczba ta **zwiększyła się o 4%**. W stosunku do lipca 2026 r. pozostawała ona na zbliżonym poziomie.

Zarejestrowane incydenty cyberbezpieczeństwa od VIII 2025 do VIII 2026



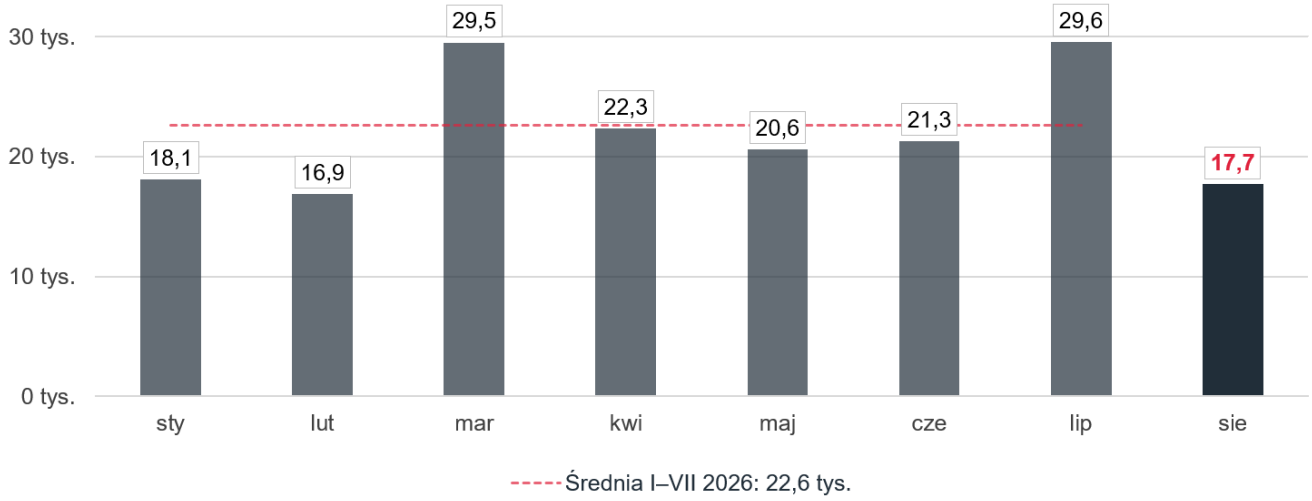
Wykres 2. Liczba zarejestrowanych incydentów od 01.08.2025 do 31.08.2026. Źródło: CERT Polska / CSIRT NASK.

Liczba incydentów zarejestrowanych w sierpniu 2026 r. wyniosła **18,9 tys.** W porównaniu z analogicznym miesiącem 2025 r. liczba incydentów w sierpniu 2026 r. **zmniejszyła się o 7%** i pozostawała poniżej średniej liczonej z 12 poprzednich miesięcy. W stosunku do lipca 2026 r. odnotowano **spadek liczby incydentów o 40%**.

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

Na Listę Ostrzeżeń wpisywane są domeny, które wprowadzają użytkowników w błąd i wyłudzają 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.

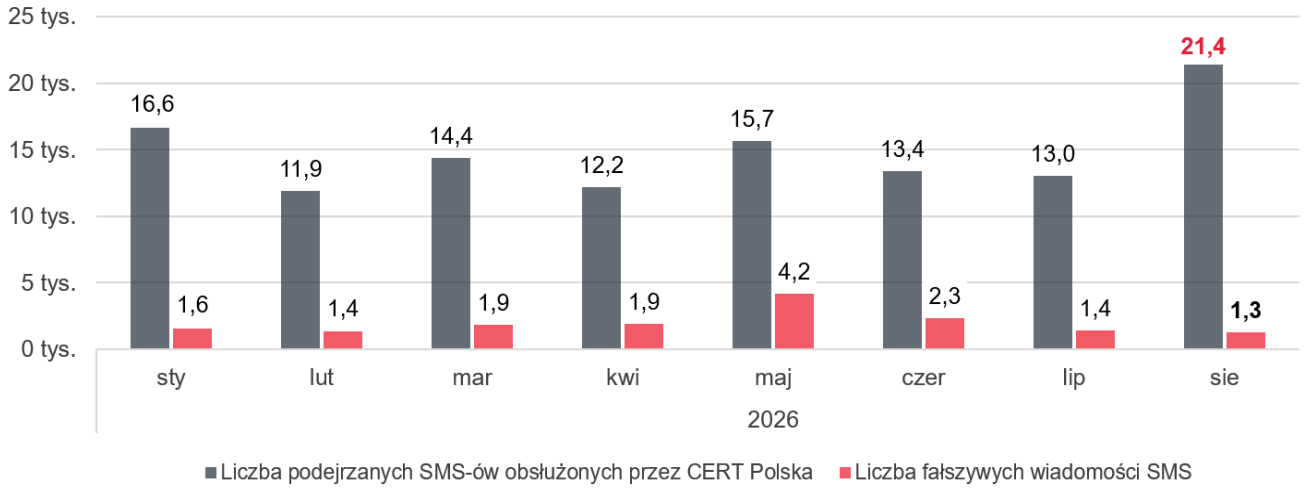


Wykres 3. Liczba nazw szkodliwych domen wpisanych na Listę Ostrzeżeń. Źródło: CERT Polska / CSIRT NASK.

Od 1 stycznia do 31 sierpnia 2026 r. na Listę Ostrzeżeń przed niebezpiecznymi stronami wpisano **176,0 tys.** szkodliwych domen, z czego w sierpniu 2026 r. dodano **17,7 tys.** nazw domen wykorzystywanych do wyłudzania danych osobowych, danych uwierzytelniających do kont bankowych i serwisów społecznościowych. Wartość ta w stosunku do lipca 2026 r. **zmniejszyła się o 40%**.

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

Od 1 stycznia do 31 sierpnia 2026 r. zespół CERT Polska zarejestrował **118,6 tys.** zgłoszeń podejrzanych SMS-ów. Liczba SMS-ów otrzymanych w sierpniu 2026 r. wyniosła **21,4 tys.** W porównaniu z lipcem 2026 r. był to **wzrost o 65%**. Wśród ogółu SMS-ów przyjętych w sierpniu 2026 r. **fałszywe 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 6%**.



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

Wzorce fałszywych wiadomości SMS I–VIII 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**. W sierpniu 2026 r., na podstawie wytworzonych przez CERT Polska wzorców fałszywych wiadomości SMS, zablokowano łącznie **17,7 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	Razem
Liczba wytworzonych wzorców	118	97	85	80	105	36	57	**94**	**672**

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

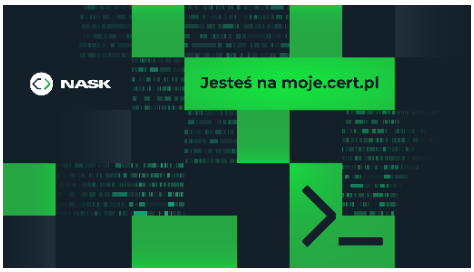
Moje.cert.pl

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 korzysta m.in. z systemów **Artemis** (skanowanie stron) i **n6** (informacje o zagrożeniach dla adresacji IP) – narzędzi pozwalających chronić dane i infrastrukturę.

W sierpniu 2026 r. w serwisie moje.cert.pl **zarejestrowało się 671 nowych użytkowników**.



W okresie od 1 do 31 sierpnia 2026 r. CERT Polska wysłał **8,1 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

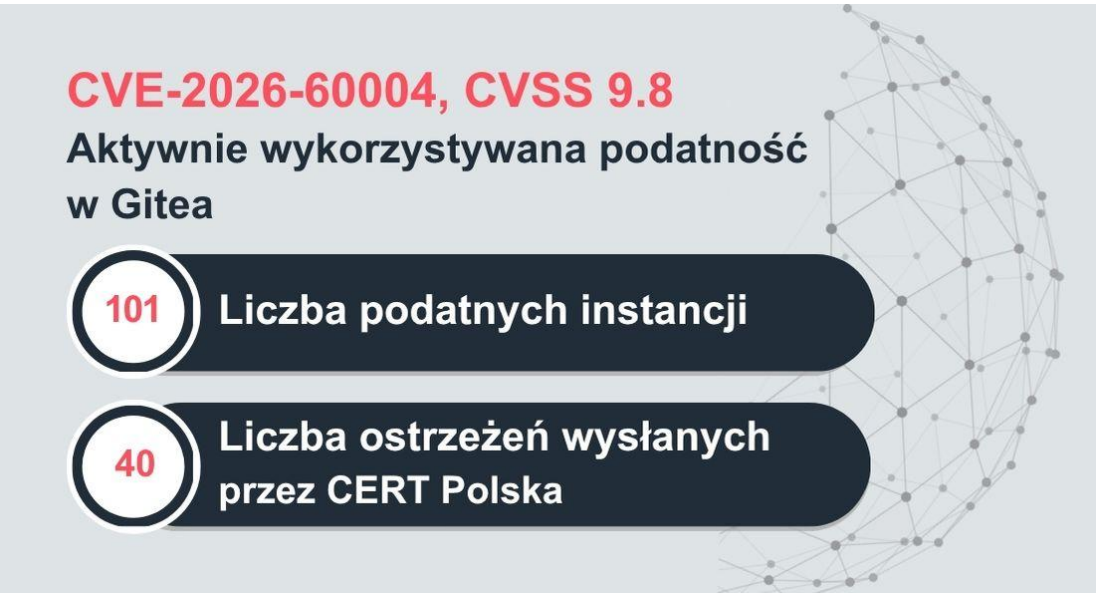
Zespół CERT Polska od sierpnia 2023 r. pełni funkcję CNA (ang. *CVE Numbering Authority*) – współtworzy bazę podatności poprzez nadawanie numerów CVE, które służą do identyfikacji i katalogowania publicznie ujawnionych podatności (więcej: CERT Polska/CNA). W sierpniu 2026 r. zespół CERT Polska nadał **33** numery CVE. Wśród wykrytych podatności znalazły się podatności w oprogramowaniu m.in. ATutor, GNU Emacs, GNU cpio, Magnolia CMS, OutSystems Service Center, dool.

Lista opublikowanych podatności dostępna jest na stronie: CERT Polska/CVE

Tabela 3. Nadane numery CVE od 1 stycznia do 31 sierpnia 2026 r.

Numery CVE w 2026	sty	lut	mar	kwi	maj	cze	lip	sie	Razem
Liczba opublikowanych numerów CVE	16	12	32	21	34	47	53	**33**	**248**

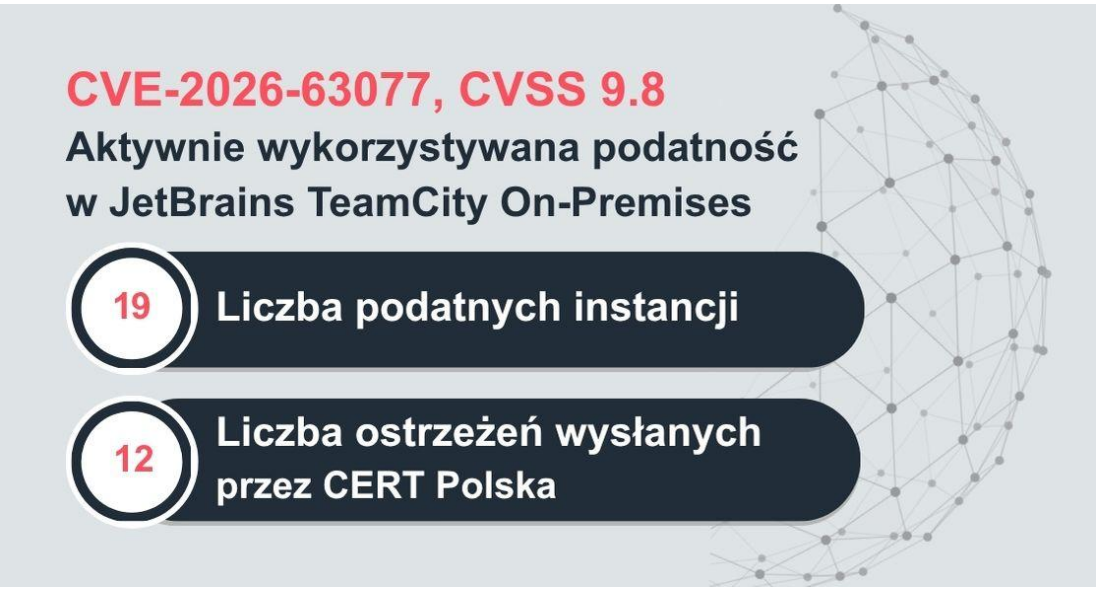
Wybrane podatności i ich wpływ na krajobraz cyberbezpieczeństwa w Polsce – VIII 2026



Krytyczna luka w funkcji porównywania zmian (diffpatch) w Gitea. Podatność umożliwia osobie posiadającej uprawnienia do zapisu do repozytorium umieszczenie złośliwego hooka Git i wykonanie dowolnych poleceń z uprawnieniami usługi Gitea. W instalacjach z otwartą rejestracją atakujący może samodzielnie utworzyć konto i repozytorium, przez co wykorzystanie podatności nie wymaga wcześniejszego dostępu. Luka jest aktywnie wykorzystywana i znajduje się w katalogu CISA KEV. Możliwe skutki obejmują przejęcie serwera, kradzież kodu i poświadczeń oraz ingerencję w procesy CI/CD. Podatne są wersje 1.17.0–1.27.0.

Rekomendujemy natychmiastową aktualizację do wersji 1.27.1 lub nowszej, wyłączenie otwartej rejestracji oraz sprawdzenie hooków, nowych kont i procesów uruchamianych przez usługę.

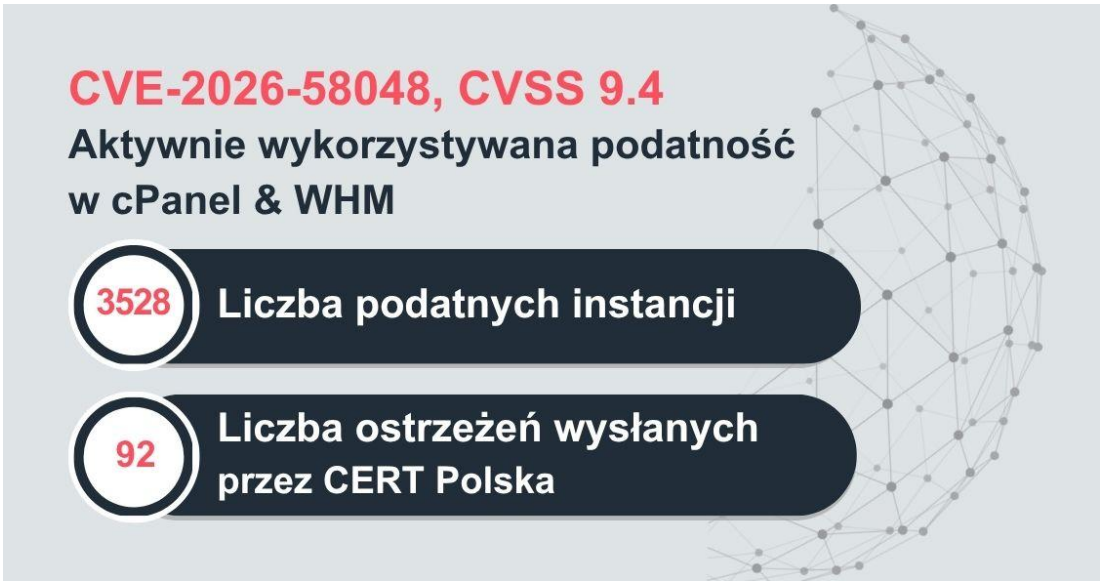
Więcej: https://www.cisa.gov/news-events/alerts/2026/08/25/cisa-adds-one-known-exploited-vulnerability-catalog, https://github.com/go-gitea/gitea/security/advisories/GHSA-rcr6-4jqh-j84m



Krytyczna luka typu unsafe deserialization w protokole komunikacji agentów TeamCity. Atakujący, mając dostęp HTTP lub HTTPS do podatnego serwera, może bez uwierzytelnienia przesłać złośliwe dane i wykonać dowolne polecenia systemowe z uprawnieniami procesu TeamCity. Skutkiem może być kradzież konfiguracji i zapisanych poświadczeń, modyfikacja wyników kompilacji oraz naruszenie całego łańcucha CI/CD.

Podatność jest aktywnie wykorzystywana i została dodana do katalogu CISA KEV. Rekomendujemy natychmiastową aktualizację do TeamCity 2025.11.7 lub 2026.1.3 albo instalację poprawki bezpieczeństwa dostępnej dla wersji od 2017.1. Należy również przeanalizować logi i listę nieautoryzowanych agentów.

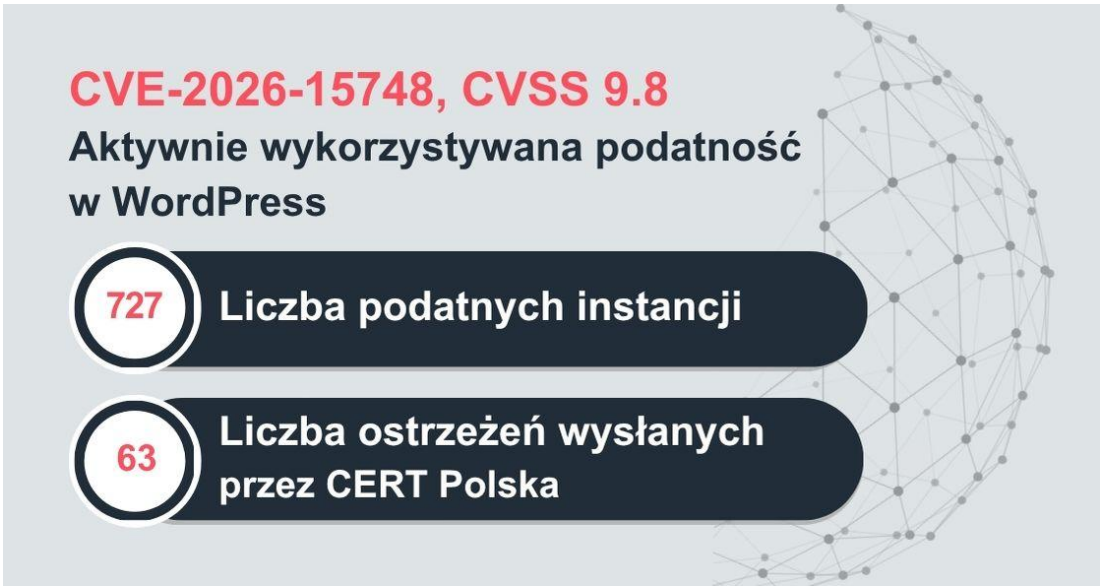
Więcej: https://content.govdelivery.com/accounts/USDHSCISA/bulletins/423c096, https://blog.jetbrains.com/teamcity/2026/08/cve-2026-63077-update



Krytyczna luka w mechanizmie zarządzania bazami danych, dotycząca wszystkich wspieranych wersji cPanel & WHM. Uwierzytelniony użytkownik posiadający dostęp do funkcji MySQL/MariaDB może wykonywać zapytania z uprawnieniami administratora bazy danych. W środowiskach hostingu współdzielonego umożliwia to dostęp do baz innych klientów, ich modyfikację lub usunięcie, a w określonych konfiguracjach – także przejęcie systemu operacyjnego serwera.

Rekomendujemy aktualizację co najmniej do wersji 11.110.0.137, 11.118.0.71, 11.126.0.78, 11.134.0.48, 11.136.0.32 lub 138.1.6 dla WP Squared. Jeśli aktualizacja nie jest możliwa, należy tymczasowo odebrać użytkownikom dostęp do funkcji MySQL.

Więcej: https://support.cpanel.net/hc/en-us/articles/42285745783703-Security-CVE-2026-58048-Database-Privilege-Escalation, https://www.csa.gov.sg/alerts-and-advisories/alerts/al-2026-097



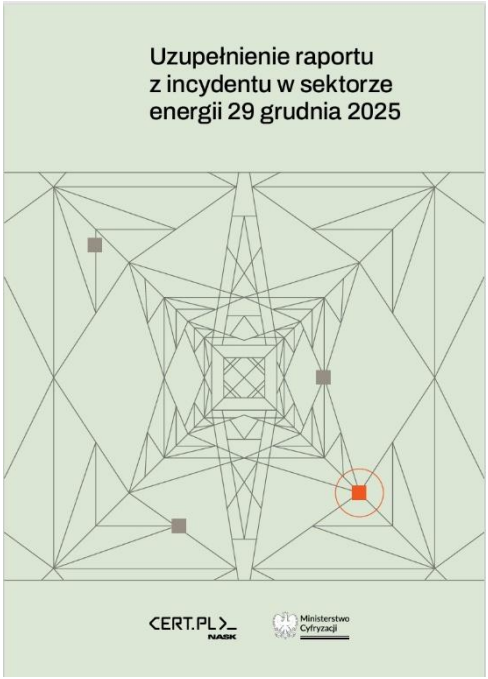
We wtyczce do systemu WordPress wykryto krytyczną podatność umożliwiającą przesyłanie na serwer plików dowolnego typu bez konieczności logowania. Nieprawidłowa walidacja rozszerzeń

i typów MIME pozwala atakującemu sfałszować konfigurację pola formularza oraz przesłać wykonywalny plik PHP. Uruchomienie takiego pliku prowadzi do zdalnego wykonania kodu, przejęcia witryny, kradzieży danych oraz instalacji trwałego dostępu. Podatne są wszystkie wersje Forminator Forms do 1.56.1 włącznie.

Rekomendujemy natychmiastową aktualizację do wersji 1.56.2 lub nowszej oraz sprawdzenie katalogów przesyłanych plików pod kątem nieautoryzowanych skryptów.

Więcej: https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/forminator/forminator-forms-1561-unauthenticated-arbitrary-file-upload-via-forged-upload-field-configuration

Wybrane informacje



8 sierpnia zespół CERT Polska opublikował **„Uzupełnienie raportu z incydentu w sektorze energii 29 grudnia 2025”**. Pierwszy raport, który ukazał się w styczniu 2026 r., zawiera szczegółową analizę techniczną oraz przebieg skoordynowanych ataków w polskiej cyberprzestrzeni, przeprowadzonych pod koniec 2025 r. Zaatakowano wówczas ponad 30 farm wiatrowych i fotowoltaicznych, spółkę prywatną z sektora produkcyjnego oraz elektrociepłownię dostarczającą ciepło dla prawie pół miliona odbiorców w Polsce. Równolegle miał miejsce jeszcze jeden incydent – w mniejszej elektrociepłowni dostarczającej ciepło dla 50 tys. mieszkańców. Trwające ponad trzy miesiące śledztwo doprowadziło do zidentyfikowania nieobserwowanego dotychczas wektora ataku w postaci prywatnego APN. W opublikowanym teraz uzupełnieniu raportu zespół CERT Polska opisał przebieg tego incydentu oraz sposoby na zatarcie śladów wykorzystane przez atakujących, a także podał rekomendacje dla podmiotów korzystających z rozwiązań opartych na prywatnym APN.

Więcej: cert.pl/Uzupełnienie raportu z incydentu w sektorze energii w grudniu 2025 roku

W sierpniu **zespół CERT Polska** publikował w swoich mediach społecznościowych posty w ramach cyklu „Wakacyjny parasol CERT Polska" poświęconego cyberzagrożeniom, które mogą zakłócić wakacyjny wypoczynek. Posty zawierały opis scenariuszy wykorzystywanych przez cyberprzestępców oraz wskazówki, o czym trzeba pamiętać, aby nie dać się oszukać. Zwracano uwagę na oszustwa służące do wyłudzania danych, pieniędzy lub do przejęcia konta, w tym na sensacyjne artykuły, które można otworzyć dopiero po przeprowadzeniu „weryfikacji wieku" na platformie społecznościowej. Aby zwiększyć swoje bezpieczeństwo, warto włączyć uwierzytelnianie dwuskładnikowe w bankowości i usługach finansowych, w mediach społecznościowych i na komunikatorach oraz w poczcie elektronicznej.

Więcej: linkedin.com/CERT Polska/uwierzytelnianie dwuetapowe, linkedin.com/CERT Polska/phishing

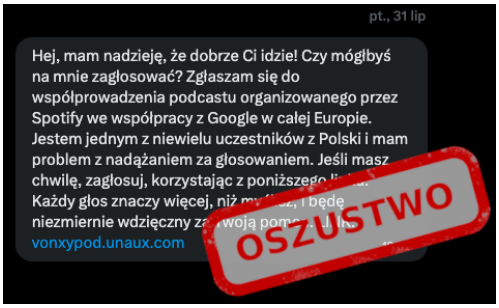
Wystąpienia ekspertów CERT Polska

- 8 sierpnia podczas konferencji DEF CON odbywającej się w Las Vegas kierownik CERT Polska opowiedział o wynikach śledztwa w sprawie incydentu z końca grudnia 2025 r. w elektrociepłowni dostarczającej ciepło dla 50 tys. mieszkańców, które doprowadziło do zidentyfikowania nieobserwowanego dotychczas wektora ataku w postaci prywatnego APN. Była to też okazja do omówienia procesu analizy incydentu przez zespół CERT Polska oraz wyzwań, które się z tym wiązały, a także do prezentacji wniosków dotyczących bezpieczeństwa prywatnych sieci APN i zarządzania incydentami na dużą skalę obejmującymi infrastrukturę krytyczną.

  Więcej: info.defcon.org/opis wystąpienia

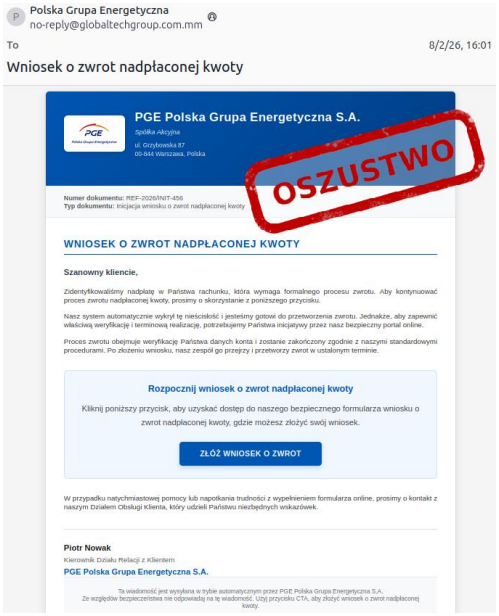
Komunikaty o zagrożeniach

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



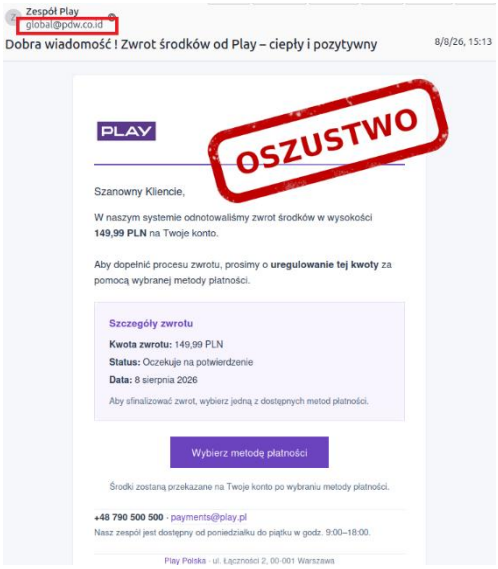
Zespół CERT Polska ostrzegał przed nową metodą stosowaną przez oszustów. Przestępcy przejmują konta WhatsApp i w imieniu ich właścicieli rozsyłają wiadomości zawierające informacje o rzekomym konkursie oraz prośbę o oddanie głosu. W wiadomości znajduje się link, za pomocą którego można oddać głos. Aby zagłosować, trzeba przejść proces „weryfikacji” przez konto WhatsApp. Weryfikacja ma polegać na wybraniu w ustawieniach opcji „Połącz urządzenie” i zeskanowanie aplikacją podstawionego kodu QR lub przepisanie kodu weryfikacyjnego. W ten sposób oszuści uzyskują dostęp do konta użytkownika i mogą je wykorzystywać do dalszych oszustw.

Aby odciąć oszustom dostęp, należy jak najszybciej zakończyć sesje logowania wszystkich urządzeń sparowanych z kontem. Można to zrobić w ustawieniach aplikacji.

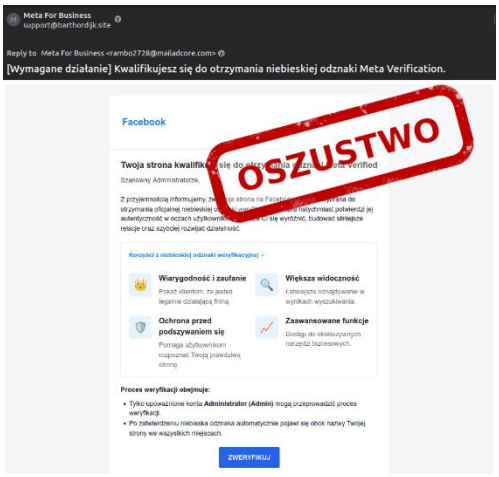


Zespół CERT Polska obserwował powrót kampanii phishingowej, w której przestępcy podszywają się pod PGE. W wiadomościach e-mail oszuści informują o rzekomej nadpłacie na rachunku użytkownika i możliwości zwrotu pieniędzy. Aby uzyskać zwrot, użytkownik ma wypełnić wniosek, do którego prowadzi link podany w wiadomości. Odnośnik kieruje na stronę podszywającą się pod panel logowania do konta. Dane wpisane przez użytkownika trafiają do cyberprzestępców.

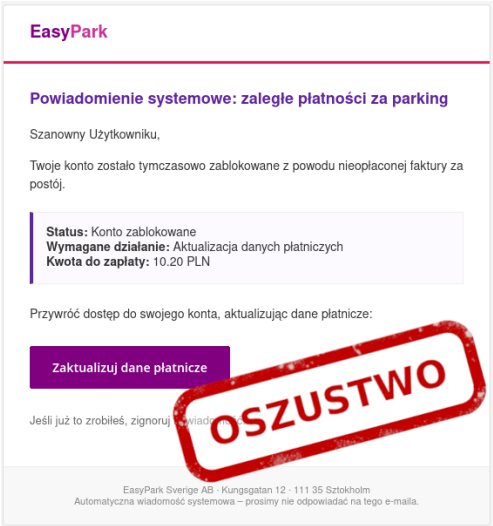
Zespół CERT Polska informował o kampanii phishingowej, w której oszuści podszywają się pod e-Urząd Skarbowy. To dobrze znany schemat, który cyberprzestępcy nieustannie wykorzystują. W wiadomościach e-mail informują, że po zakończeniu weryfikacji rocznego zeznania podatkowego za 2025 r. użytkownikowi przysługuje zwrot nadpłaconego podatku dochodowego, a następnie zachęcają do „potwierdzenia dyspozycji wypłaty". Odnośnik zawarty w wiadomości prowadzi na fałszywą stronę internetową, gdzie przestępcy próbują wyłudzić od użytkownika numer PESEL, dane osobowe oraz dane karty płatniczej.



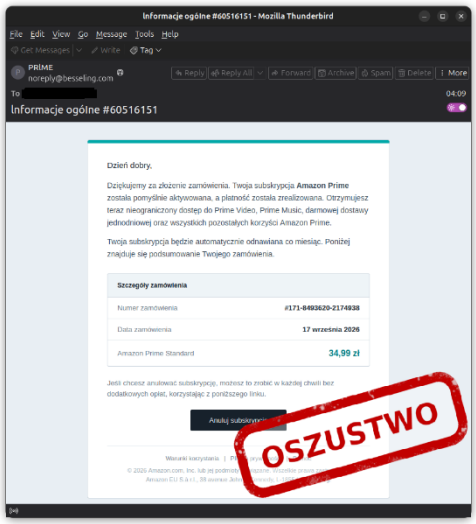
Zespół CERT Polska obserwował kampanię phishingową skierowaną do klientów jednego z operatorów sieci komórkowej. Oszuści wysyłają wiadomości e-mail, w których informują o rzekomo przysługującym użytkownikowi zwrocie środków. W wiadomości znajduje się przycisk „Wybierz metodę płatności" z linkiem przenoszącym na stronę imitującą witrynę operatora. Tam oszuści próbują wyłudzić dane osobowe oraz dane karty płatniczej użytkownika.



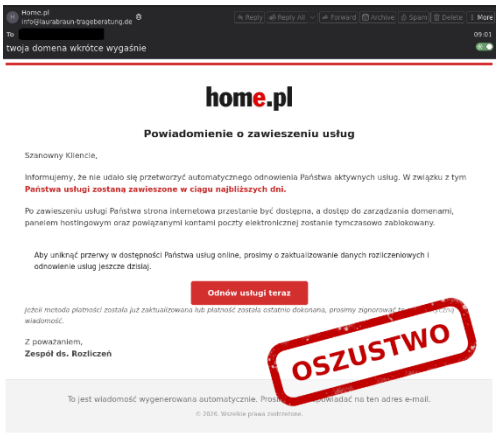
Zespół CERT Polska obserwował kampanię phishingową wymierzoną we właścicieli stron na Facebooku. Oszuści podszywają się pod administrację platformy. Wysyłają wiadomości, w których informują o rzekomej możliwości otrzymania odznaki Meta Verified po przeprowadzeniu procesu weryfikacji. Odnośnik zawarty w wiadomości prowadzi do strony, która łudząco przypomina oficjalny serwis Facebooka. Tam znajduje się formularz, który służy oszustom do wyłudzania danych logowania do konta. Pozyskane dane pozwalają cyberprzestępcom przejąć konto i wykorzystać je do dalszych oszustw.



Zespół CERT Polska przestrzegał przed kampanią phishingową, w której cyberprzestępcy rozsyłają fałszywe powiadomienia systemowe o zaległej płatności za parking. W wiadomości e-mail znajduje się informacja o symbolicznej kwocie zaległości i zablokowaniu konta. Aby przywrócić dostęp do konta, użytkownik ma zaktualizować dane płatnicze. Odnośnik zawarty w wiadomości prowadzi na fałszywą stronę, która służy do wyłudzania danych osobowych i danych karty płatniczej.



Zespół CERT Polska obserwował kampanię phishingową, w której oszuści wykorzystują popularną usługę Amazon Prime. W wiadomościach dziękują za złożenie zamówienia i informują, że subskrypcja została aktywowana, a płatność – zrealizowana. Podają też szczegóły rzekomo złożonego zamówienia. Jednocześnie informują, że użytkownik może anulować subskrypcję – w każdej chwili i bez dodatkowych opłat – za pomocą wskazanego odnośnika. Link prowadzi na fałszywą stronę internetową przypominającą serwis Amazon. Tam oszuści próbują wyłudzić od użytkownika jego adres e-mail lub numer telefonu oraz dane karty płatniczej.



Zespół CERT Polska informował o trwającej kampanii, w której cyberprzestępcy wykorzystują wizerunki dostawców usług hostingowych. W wiadomościach e-mail informują odbiorców, że ich strony zostaną zawieszone w ciągu najbliższych dni w związku z tym, że nie udało się przetworzyć automatycznego odnowienia usług. W wiadomości znajduje się przycisk „Odnów usługi teraz” z linkiem prowadzącym do fałszywego serwisu logowania. Po wpisaniu danych logowania użytkownik jest kierowany do kolejnego formularza, w którym ma wprowadzić dane karty płatniczej. Dane użytkownika mogą posłużyć oszustom do kradzieży pieniędzy z konta oraz do dalszych oszustw.

Zespół CERT Polska obserwował kampanię phishingową wymierzoną w użytkowników usług Microsoft. Oszuści rozsyłają wiadomości e-mail o rzekomo zbliżającym się terminie wygaśnięcia hasła i zachęcają do jego „aktualizacji”. W wiadomości znajduje się link prowadzący do strony imitującej panel logowania do konta Microsoft. Dane wpisane przez użytkownika mogą zostać użyte przez cyberprzestępców do uzyskania dostępu do konta i powiązanych z nim usług oraz do przeprowadzenia dalszych ataków.

Więcej: Facebook/CERT Polska, X/CERT Polska, moje.cert.pl/komunikaty, LinkedIn/CERT Polska

Opis najczęściej występujących kampanii – VIII 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 wypłaty zainwestowanych pieniędzy. Celem oszustów jest wyłudzenie środków finansowych.

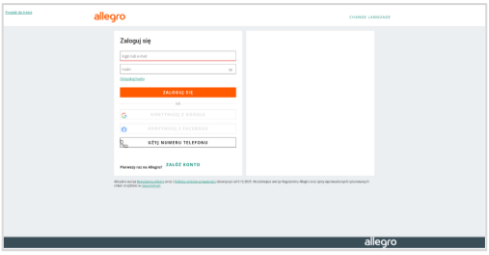
Fałszywe strony serwisu Gazeta.pl

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 serwisu WP.pl

Zespół CERT Polska obserwował kampanię phishingową, w której wykorzystywany jest wizerunek serwisu WP.pl. Na fałszywych stronach internetowych znajdują się artykuły na temat inwestycji, na których rzekomo można zarobić z dużym zyskiem.

Fałszywe strony Allegro

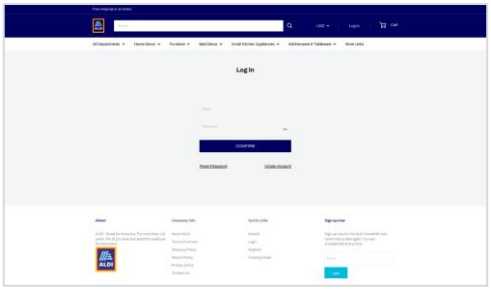


Zespół CERT Polska obserwował wzmożoną kampanię phishingową, w której oszuści wykorzystującą wizerunek platformy Allegro. Na fałszywych stronach internetowych znajduje się panel logowania do tego serwisu służący do wyłudzania danych uwierzytelniających od użytkowników Allegro.

Fałszywe strony OLX

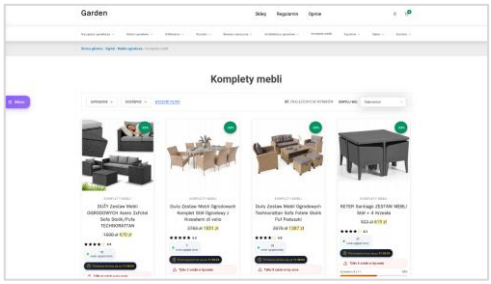
Zespół CERT Polska zarejestrował incydenty, w których atakujący za pośrednictwem stron internetowych podszywają się pod serwis OLX. Panel logowania do tego serwisu służy do wyłudzania od użytkowników danych uwierzytelniających.

Fałszywe strony sklepów internetowych wykorzystujących markę ALDI



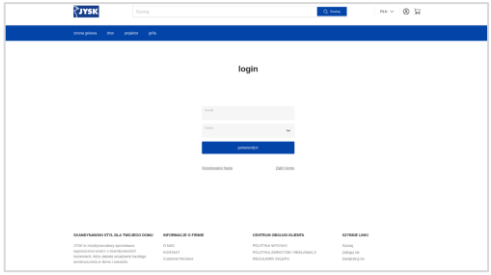
Zespół CERT Polska obserwował incydenty, w których oszuści tworzą fałszywe sklepy internetowe z wykorzystaniem wizerunku sieci sklepów ALDI. Celem oszustów jest wyłudzenie od użytkowników danych uwierzytelniających oraz kradzież środków finansowych.

Fałszywe strony sklepów internetowych



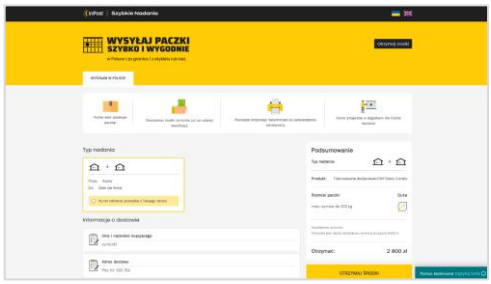
Zespół CERT Polska zarejestrował kampanię, w której oszuści tworzą fałszywe sklepy internetowe, oferujące towary w atrakcyjnych cenach, i wykorzystują je do wyłudzania danych uwierzytelniających oraz kradzieży środków finansowych.

Fałszywe strony internetowe sieci handlowej JYSK



Zespół CERT Polska rejestrował incydenty, w których oszuści wykorzystują wizerunek marki JYSK.
Na fałszywych stronach internetowych znajduje się panel logowania służący do wyłudzania od klientów danych uwierzytelniających.

Fałszywe strony 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 strony kanału TVN

Zespół CERT Polska obserwował incydenty, w których oszuści wykorzystują wizerunek kanału telewizyjnego TVN. Na fałszywych stronach internetowych znajdują się artykuły na temat inwestycji, na których rzekomo można zarobić z dużym zyskiem.