Log4Shell

Informacja nt. obsługi incydentu cyberbezpieczeństwa

CSIRT GOV | CSIRT MON | CSIRT NASK

17 grudnia 2021
Autor: Opracowanie zbiorcze

Log4Shell

Informacja nt. obsługi incydentu cyberbezpieczeństwa

Spis treści

Wprowadzenie

Niniejsze opracowanie zawiera informacje o incydencie cyberbezpieczeństwa związanym z ujawnieniem podatności w powszechnie stosowanej bibliotece oprogramowania oraz przebieg jego obsługi przez Zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT) działające na poziomie krajowym w rozumieniu ustawy o krajowym systemie cyberbezpieczeństwa z dnia 5 lipca 2018 roku.

Opis incydentu

Powszechnie wykorzystywana, wieloplatformowa biblioteka Apache Log4j posiada krytyczną lukę, umożliwiającą zdalne wykonanie kodu (ang. Remote Code Execution - RCE). Podatność ta, której nadano oznaczenie CVE-2021-44228, przy dodatkowych warunkach, pozwala atakującemu na przejęcie pełnej kontroli nad serwerem lub stacją roboczą. Warunkiem koniecznym - w tym wypadku - jest implementacja oprogramowania w taki sposób, że system zapisuje w dzienniku zdarzeń informacje, na które ma wpływ atakujący (użytkownik), co nie jest rzadkością.

Ze względu na szerokie zastosowanie biblioteki w wielu aplikacjach i usługach oraz łatwość wykorzystania podatności, obsłudze incydentu nadano najwyższy priorytet we wszystkich zespołach CSIRT poziomu krajowego.

Zagrożenie dotyczy wszystkich usług oraz systemów wykorzystujących Java Virtual Machine (JVM) i korzystających z biblioteki Apache Log4j w wersjach od 2.0 do 2.14.1 włącznie.

Ponieważ podatność pozwala na wykonanie kodu na podatnej maszynie - **incydent**, przez społeczność zajmującą się cyberbezpieczeństwem, **został nazwany Log4Shell**.

Podjęte działania

Pierwsze informacje o wykrytej podatności pojawiły się 10 grudnia 2021 roku a zespoły CSIRT poziomu krajowego niezwłocznie podjęły działania, stosownie do swoich obszarów odpowiedzialności (ang. constituency):

1. W CSIRT NASK przystąpiono do opracowania polskojęzycznego artykułu wraz z rekomendacjami, co skutkowało opublikowaniem rozbudowanego opisu krytycznej podatności. Artykuł zawiera zarówno metody weryfikacji, czy podatność istnieje w wykorzystywanych systemach, jak i szczegółowe rekomendacje postępowania i jest dostępny pod adresem:

   https://cert.pl/posts/2021/12/krytyczna-podatnosc-w-bibliotece-apache-log4j/ [1]

   Wraz z publikacją artykułu zespół rozpoczął równoległą dystrybucję ostrzeżeń poprzez media społecznościowe (Twitter i LinkedIn) z odniesieniem do artykułu, celem dotarcia do jak największej liczby odbiorców.

2. Równocześnie Zespół CSIRT GOV wydał ostrzeżenie informujące o krytycznej podatności i zarekomendował zapoznanie się z informacjami przygotowanymi na stronie Zespołu CSIRT NASK (pkt.1.) jako element holistycznego działania Krajowego Systemu Cyberbezpieczeństwa.

3. W tym samym czasie zespół CSIRT MON pracował **nad analizą podatności** pod kątem jej występowania i możliwości wykorzystania **w zasobach Resortu Obrony Narodowej**, wydaniem stosownych zaleceń i komunikatów, wprowadzeniem środków zaradczych, a także działań detekcyjnych, co skutkowało opublikowaniem poprzez oficjalny kanał społecznościowy komunikatu informującego o zaistniałym incydencie, jak również wysłaniem komunikatu ostrzegawczego do jednostek i komórek organizacyjnych MON odpowiedzialnych za eksploatację systemów teleinformatycznych, a rekomendacje co do działań mających na celu minimalizację skutków oddziaływania incydentu zawarto w „Zaleceniach Szefa CSIRT MON".

4. Ostrzeżenie dystrybuowano także w ramach Systemu S46[2].

5. Dbając o wymiar międzynarodowy w zakresie obsługi incydentu, wiadomości o podatności były na bieżąco konsultowane w ramach **CSIRTs Network**, gdzie europejskie zespoły CSIRT wymieniały się informacjami o zagrożeniu oraz planowanych do podjęcia działaniach. Istotność problemu spowodowała, iż zwołane zostało nadzwyczajne spotkanie **CSIRTs Network**, gdzie Krajowy System Cyberbezpieczeństwa reprezentowany był przez CSIRT NASK.

6. Mając świadomość **zagrożenia dla infrastruktury krytycznej oraz systemów rządowych**, CSIRT GOV przesyłał kolejne informacje oraz rekomendacje,

[1] Od momentu publikacji artykułu na stronie do godziny **19:00 dn.15.12.2021** artykuł został odwiedzony ponad **30 tysięcy razy**

[2] działającego zgodnie z art. 46 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa

a z uwagi na szerokie wykorzystanie podatnej biblioteki w aplikacjach biznesowych i serwerach usług, a także serwisach chmurowych, poziom zagrożenia został uznany jako bardzo wysoki. Rekomendacje wskazywały m.in. na pilną weryfikację użytkowanych usług systemowych, zwłaszcza dostępnych z sieci Internet, a także w ramach dostawców rozwiązań chmurowych. Przekazano informacje dot. wykazów podatnych produktów, które w przypadku identyfikacji, należało poddać procedurze konsultacji z danym producentem w zakresie bezpieczeństwa ich dalszego użytkowania.

Zaznaczono, iż nie jest to lista zamknięta. W każdym przypadku innych usług zarekomendowano sprawdzenie stosownych stron producenta oprogramowania, a w przypadku braku dostępnych aktualizacji i rekomendacji producenta, zarekomendowano rozważenie wyłączenia dostępu podatnej usługi w sieci Internet, jeśli nie wpłynęłoby to na ciągłość działania instytucji, jak również zarekomendowano monitorowanie dzienników zdarzeń serwerów usług w celu poszukiwania potencjalnych prób wykorzystania podatności.

Załączono wskazania do przydatnych w tym celu narzędzi i przykładowe wzorce poszukiwań. Ponadto poinformowano o wzmożonych próbach skanowania serwerów i próbach wykorzystywania tej podatności, a do ostrzeżeń załączona została lista adresów IP, które zostały zidentyfikowane jako skanery ukierunkowane na jej poszukiwanie. Rekomendowano sprawdzenie wskazanych adresów IP, czy nie występują w logach aplikacyjnych i wdrożenie reguł na systemach zaporowych.

Zwrócono się także o przesłanie zwrotnie informacji dotyczących przeprowadzenia weryfikacji usług pod kątem podatności w zakresie stanu wdrożenia zaleceń producenta lub w przypadku ich braku innych środków mitygujących, zaraportowania o próbach ataku (adresy IP, artefakty połączeń do serwerów) lub zgłoszenia incydentu wykorzystania podatności.

7. Równocześnie, dzięki działaniom CSIRT NASK, udało się zidentyfikować dwa **podatne podmioty będące Operatorem Usługi Kluczowej**. Zostały one powiadomione i skutecznie usunęły podatność.
8. Wsparciem dla CSIRT poziomu krajowego stanowiła również prowadzona zacieśniona współpraca z CSIRT KNF (sektorowym zespołem cyberbezpieczeństwa), który rozesłał do sektora finansowego rekomendacje z naciskiem, że **działania powinny zostać podjęte natychmiast**. CSIRT KNF zidentyfikował dodatkowe 3 podmioty z własnego sektora podatne na atak z zewnątrz.
9. Kontynuując akcję powszechnego ostrzegania o zagrożeniu, CSIRT NASK, w ramach listy osób kontaktowych zgłoszonych trybie art. 9 ust 2, art. 22 ust. 1 pkt. 5 ustawy o Krajowym Systemie Cyberbezpieczeństwa, rozesłał dodatkowe ostrzeżenia do podmiotów będących w obszarze jego odpowiedzialności. Do **2976 podmiotów zostało wysłanych łącznie 6463 indywidualnych powiadomień**

(unikatowych adresów poczty elektronicznej). Na dzień **15 grudnia 2021** zespół otrzymał informację zwrotną od **348 powiadomionych podmiotów**.

10. Aktywizując działania ponadgraniczne został nawiązany kontakt z Dutch Institute for Vulnerability Disclosure (DIVD CSIRT), społecznością COVID-19 CTI League oraz firmami komercyjnymi, co do których pojawiły się doniesienia, że prowadzą aktywne skanowania pod kątem występowania podatności. Na tę chwilę organizacje te nie wykryły jeszcze żadnych podatnych systemów w Polsce.
11. Dnia **14 grudnia 2021** Zespół CSIRT NASK otrzymał w ramach wymiany danych w **CSIRTs Network** informacje o **52 podatnych maszynach** w z adresami IP lokalizowanymi geograficznie w Polsce. Zidentyfikowane podmioty zostały powiadomione.
12. W odpowiedzi na powyżej wskazywane ostrzeżenia i rekomendacje podmioty, na które mógł mieć wpływ incydent, zgłaszają podjęcie następujących działań:
    - podejmowanie działań mitygujących w konsultacji z dostawcami oraz producentami wykorzystywanych usług;
    - wyszukiwanie obecności podatnych bibliotek we wszystkich dostępnych systemach;
    - aktualizacja biblioteki do najnowszej wersji;
    - monitoring bezpieczeństwa infrastruktury teleinformatycznej w instytucji;
    - analiza dzienników zdarzeń pod kątem możliwego wykorzystania podatności;
    - wprowadzenie dodatkowych zabezpieczeń sieciowych.
13. Ponadto, w ramach działań prewencyjnych, dokonano przeglądu mechanizmów bezpieczeństwa i **objęto dodatkowym monitorowaniem zasoby najbardziej narażone na potencjalne ataki** z wykorzystaniem podatności CVE-2021-44228.

Rekomendacje

Zespoły CSIRT poziomu krajowego wskazują dwa kierunki działań związanych z obsługą podatności przez uczestników krajowego systemu cyberbezpieczeństwa:

- podjęcie działań naprawczych (aktualizacja biblioteki, współpraca z producentem) lub ograniczenie ryzyka (np. poprzez reguły blokujące, odłączenie usługi, wyłączenie Messages Lookup);
- podjęcie działań detekcyjnych (przeszukiwanie dzienników zdarzeń i innych artefaktów, monitoring procesów i ruchu sieciowego).

Działania detekcyjne należy prowadzić w sposób ciągły. Podatność pozostanie w wadliwych bibliotekach i nie ma pewności jakie oprogramowanie będzie korzystało z tych bibliotek - np. przywrócony system z kopii bezpieczeństwa, czy nowo zainstalowana długo nieużywana aplikacja.

Podsumowanie

Podejmowane działania przez zespoły CSIRT poziomu krajowego, choć prowadzone niezależnie (każdy w zakresie swojej odpowiedzialności), to oparte na wspólnej, wymienianej na bieżąco, wiedzy doprowadziły do sprawnej obsługi incydentu.

Zespoły CSIRT poziomu krajowego nadal będą prowadziły identyfikację podatnych systemów, dystrybuowały ostrzeżenia, a także udzielały wsparcia podmiotom w zakresie wdrażania działań naprawczych i zabezpieczających. Opublikowany na stronie https://cert.pl/posts/2021/12/krytyczna-podatnosc-w-bibliotece-apache-log4j/ artykuł jest systematycznie aktualizowany w miarę pojawiania się nowych rekomendacji i narzędzi umożliwiających mitygację zmaterializowanego zagrożenia.