

Joomla 0day session.php

2024-04-25 07:05:28

Wydruk artykułu FAQ

Kategoria:	Hosting ITL::Bezpieczeństwo	Ostatnia aktualizacja:	2015-12-18 11:36:28
Status:	publiczny (dla wszystkich)		
Język:	pl		

Słowa kluczowe

joomla 0day

Objawy (publiczny)

Od połowy grudnia dokonywane są ataki 0day na Joomla poprzez lukę w obsłudze sesji i nagłówka User-Agent.

Problem (publiczny)

Joomla w wersjach od 1.5 do 3.4.5 posiada lukę w obsłudze sesji w pliku `libraries/joomla/session/session.php`. Ataki dokonywane są w sposób zautomatyzowany i masowy. Atakujący są w stanie wstrzyknąć do plików strony dowolny kod PHP (backdoor). Niestety starsze wersje (1.5-2.5) nie mają już oficjalnego wsparcia, ani oficjalnych aktualizacji. Zabezpieczenia należy zaaplikować samodzielnie.

Więcej o tej luce można dowiedzieć się na tej stronie:

[1]<http://news.softpedia.com/news/joomla-3-4-6-fixes-zero-day-remote-execution-bug-used-in-the-wild-497599.shtml>

Neooficjalne wsparcie dla starszych wersji Joomla:

[2]https://docs.joomla.org/Security_hotfixes_for_Joomla_EOL_versions

[1] <http://news.softpedia.com/news/joomla-3-4-6-fixes-zero-day-remote-execution-bug-used-in-the-wild-497599.shtml>

[2] https://docs.joomla.org/Security_hotfixes_for_Joomla_EOL_versions

Rozwiązanie (publiczny)

Przygotowaliśmy nieoficjalne patche do kilku wersji Joomla, w formacie unified diff, łatwe do zaaplikowania.

Prosimy zaaplikować patch w odpowiedniej wersji.

Patch można zaaplikować np. w ten sposób na serwerze shell:

```
$ cd {Joomla_DIR}
$ patch -p0 < ~/joomla.zeroday.v3.patch
```

Wersje patchy:

joomla.zeroday.v3.patch - wersja Joomla 2.5-3.*

joomla.zeroday.v17.patch - Joomla 1.7

joomla.zeroday.v15.patch - Joomla 1.5

Uwaga: powyższy opis dotyczy tylko usunięcia oryginalnej luki.

Należy bezwzględnie sprawdzić, czy strona nie została już zainfekowana, np. przez porównanie plików z backupem. Oczywiście w przypadku infekcji, należy wyczyścić kod z backdoorów:

[1]<https://support.intertele.pl/otrs/public.pl?Action=PublicFAQZoom;ItemID=4>

[1] <https://support.intertele.pl/otrs/public.pl?Action=PublicFAQZoom;ItemID=4>