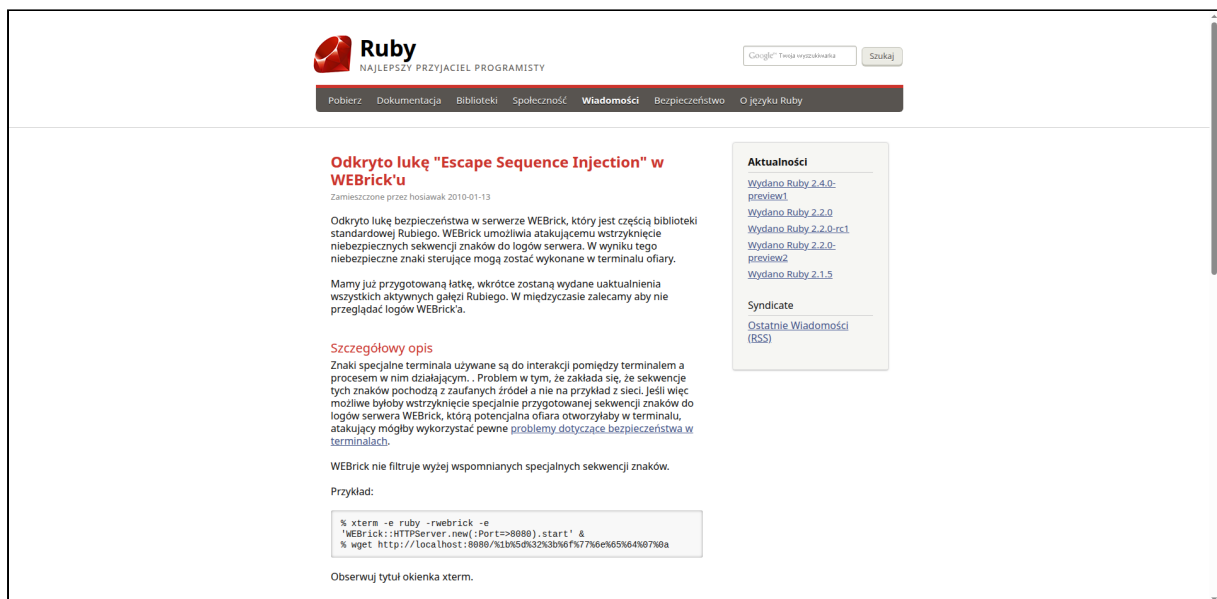


PRESS REVIEW ARCHIVE

Digital Media Monitoring & Documentation Service

Source URL:	https://www.ruby-lang.org/pl/news/2010/01/13/odkryto-luk-escape-sequence-injection-w-webricku/
Archived Date:	August 15, 2025 at 15:19
Published:	August 01, 2025
Document Type:	Web Page Archive
Wayback Machine:	https://web.archive.org/web/*/https://www.ruby-lang.org/pl/news/2010/01/13/odkryto-luk-escape-sequence-injection-w-webricku/

Page Screenshot



Odkryto lukę "Escape Sequence Injection" w WEBrick'u

Zamieszczone przez hosiawak 2010-01-13

Odkryto lukę bezpieczeństwa w serwerze WEBrick, który jest częścią biblioteki standardowej Rubiego. WEBrick umożliwia atakującemu wstrzyknięcie niebezpiecznych sekwencji znaków do logów serwera. W wyniku tego niebezpieczne znaki sterujące mogą zostać wykonane w terminalu ofiary.

Mamy już przygotowaną łatkę, wkrótce zostaną wydane uaktualnienia wszystkich aktywnych gałęzi Rubiego. W międzyczasie zalecamy aby nie przeglądać logów WEBrick'a.

Szczegółowy opis

Znaki specjalne terminala używane są do interakcji pomiędzy terminalem a procesem w nim działającym. Problem w tym, że zakłada się, że sekwencje tych znaków pochodzą z zaufanych źródeł a nie na przykład z sieci. Jeśli więc możliwe byłoby wstrzyknięcie specjalnie przygotowanej sekwencji znaków do logów serwera WEBrick, którą potencjalna ofiara otworzyłaby w terminalu, atakujący mógłby wykorzystać pewne [problemy dotyczące bezpieczeństwa w terminalach](#).

WEBrick nie filtruje wyżej wspomnianych specjalnych sekwencji znaków.

Przykład:

```
% xterm -e ruby -rwebrick -e  
'WEBrick::HTTPServer.new(:Port=>8080).start' &  
% wget http://localhost:8080/%1b%5d%32%3b%6f%77%6e%65%64%07%0a
```

Obserwuj tytuł okienka xterm.

Wersje Rubiego, których ten problem dotyczy

- Ruby 1.8.6 patchlevel 383 i wszystkie poprzednie wersje
- Ruby 1.8.7 patchlevel 248 i wszystkie poprzednie wersje
- Wersje deweloperskie Ruby 1.8 (1.8.8dev)
- Ruby 1.9.1 patchlevel 376 i wszystkie poprzednie wersje
- Wersje deweloperskie Ruby 1.9 (1.9.2dev)

Poprawki

- Poprawki dla 1.8.6, 1.8.7, oraz 1.9.1 znajdują się poniżej.
 - 1.8.7 patch-level 249 naprawia ten problem. Użytkowników 1.8.7 zachęca się do aktualizacji.
 - <https://cache.ruby-lang.org/pub/ruby/1.8/ruby-1.8.7-p249.tar.gz>
 - <https://cache.ruby-lang.org/pub/ruby/1.8/ruby-1.8.7-p249.tar.bz2>
 - <https://cache.ruby-lang.org/pub/ruby/1.8/ruby-1.8.7-p249.zip>
 - 1.9.1 patch-level 378 naprawia ten problem. Użytkowników 1.9.1 zachęca się do aktualizacji.
 - <https://cache.ruby-lang.org/pub/ruby/1.9/ruby-1.9.1-p378.tar.gz>
 - <https://cache.ruby-lang.org/pub/ruby/1.9/ruby-1.9.1-p378.tar.bz2>
 - <https://cache.ruby-lang.org/pub/ruby/1.9/ruby-1.9.1-p378.zip>
 - 1.8.6 patch-level 388 naprawia ten problem. Użytkowników 1.8.6 zachęca się do aktualizacji.

Aktualności

[Wydano Ruby 2.4.0-preview1](#)
[Wydano Ruby 2.2.0](#)
[Wydano Ruby 2.2.0-rc1](#)
[Wydano Ruby 2.2.0-preview2](#)
[Wydano Ruby 2.1.5](#)

Syndicate

[Ostatnie Wiadomości \(RSS\)](#)

- <https://cache.ruby-lang.org/pub/ruby/1.8/ruby-1.8.6-p388.tar.gz>
 - <https://cache.ruby-lang.org/pub/ruby/1.8/ruby-1.8.6-p388.tar.bz2>
 - <https://cache.ruby-lang.org/pub/ruby/1.8/ruby-1.8.6-p388.zip>
- Wersje deweloperskie prosimy zaktualizować do najnowszej wersji.

Podziękowania

Podziękowania należą się Giovanni "evilaliv3" Pellerano, Alessandro "jekil" Tanasi, oraz Francesco "ascii" Ongaro za odkrycie tej luki.

[Pobierz](#) [Dokumentacja](#) [Biblioteki](#) [Społeczność](#) [Wiadomości](#) [Bezpieczeństwo](#) [O języku Ruby](#)

Ta strona w innych językach: [Български](#), [Deutsch](#), [English](#), [Español](#), [Français](#), [Bahasa Indonesia](#), [Italiano](#), [日本語](#), [한국어](#), [polski](#), [Português](#), [Русский](#), [Türkçe](#), [Tiếng Việt](#), [简体中文](#), [繁體中文](#).

[Logo Rubiego](#) jest Zastrzeżone © 2006, Yukihiro Matsumoto; licencjonowane na warunkach [CC BY-SA 2.5](#).

Serwis powstał w języku Ruby przy użyciu [Jekyll](#). Utrzymaniem serwisu zajmuje się społeczność Rubiego. Projekt strony [Jason Zimdars](#). Proszę udzielić nam wsparcia na [GitHub](#) lub skontaktuj się z naszym [webmasterem](#) jeśli masz jakieś pytania lub komentarze dotyczące tego serwisu.