

# PRESS REVIEW ARCHIVE

Digital Media Monitoring & Documentation Service

**Source URL:** <https://security.snyk.io/vuln/SNYK-RUBY-WEBRICK-1315609>

**Archived Date:** August 15, 2025 at 15:13

**Document Type:** Web Page Archive

**Wayback Machine:** [https://web.archive.org/web/\\*/https://security.snyk.io/vuln/SNYK-RUBY-WEBRICK-1315609](https://web.archive.org/web/*/https://security.snyk.io/vuln/SNYK-RUBY-WEBRICK-1315609)

## Page Screenshot

The screenshot displays the Snyk Security page for the 'Improper Input Validation' vulnerability in the 'webrick' package. The page header includes the Snyk logo and a search bar. The main content area is titled 'Improper Input Validation' and notes that it affects 'webrick' package versions '<1.4.0.beta1'. A 'How to fix?' section advises upgrading 'webrick' to version 1.4.0.beta1 or higher. An 'Overview' section describes the vulnerability, stating that affected versions are vulnerable to improper input validation, allowing attackers to inject malicious escape sequences into logs, making it possible for dangerous control characters to be executed on a victim's terminal emulator. A 'PoC' section provides a command to reproduce the issue: `% xterm -e ruby -rwebrick -e 'WEBrick::HTTPServer.new({Port=>8080}).start' & % wget http://localhost:8080/11b45d9323b46f677b6e46564987b8a`. A 'References' section lists links to 'RedHat Bugzilla Bug', 'Ruby-Lang News', and 'Security Focus'. On the right side, a 'Severity' section shows a score of 9.8, labeled 'CRITICAL', with a 'RECOMMENDED' status. Below this, a 'Threat Intelligence' section shows 'Exploit Maturity' as 'PROOF OF CONCEPT' and 'EPSS' as '18.65% (95th percentile)'. At the bottom right, a section titled 'Do your applications use this vulnerable package?' offers a 'Test your applications' button.

**Snyk | SECURITY**

Snyk Vulnerability Database / RubyGems / webrick

Search by package name or CVE

### Improper Input Validation

Affecting [webrick](#) package, versions <1.4.0.beta1

INTRODUCED: 1 JUL 2021 [CVE-2009-4492](#) [CVE-20](#)

**How to fix?**

Upgrade [webrick](#) to version 1.4.0.beta1 or higher.

**Overview**

[webrick](#) is a HTTP server toolkit that can be configured as an HTTPS server, a proxy server, and a virtual-host server. Affected versions of this package are vulnerable to Improper Input Validation. WEBrick lets attackers to inject malicious escape sequences to its logs, making it possible for dangerous control characters to be executed on a victim's terminal emulator. This is due to data being written to a log file without sanitizing non-printable characters. Remote attackers could modify a window's title, execute arbitrary commands, or overwrite files via an HTTP request containing an escape sequence for a terminal emulator.

**PoC**

```
% xterm -e ruby -rwebrick -e 'WEBrick::HTTPServer.new({Port=>8080}).start' &
% wget http://localhost:8080/11b45d9323b46f677b6e46564987b8a
```

**References**

- [RedHat Bugzilla Bug](#)
- [Ruby-Lang News](#)
- [Security Focus](#)

**Severity**

9.8

CRITICAL

RECOMMENDED

CVSS assessment by Snyk's Security Team. [Learn more](#)

**Threat Intelligence**

Exploit Maturity

PROOF OF CONCEPT

EPSS

18.65% (95th percentile)

**Do your applications use this vulnerable package?**

In a few clicks we can analyze your entire application and see what components are vulnerable in your application, and suggest you quick fixes.

[Test your applications](#)

# Improper Input Validation

Affecting [webrick](#) package, versions `<1.4.0.beta1`

INTRODUCED: 1 JUL 2021 [CVE-2009-4492](#) ⓘ [CWE-20](#) ⓘ

## How to fix?

Upgrade `webrick` to version 1.4.0.beta1 or higher.

## Overview

[webrick](#) is a HTTP server toolkit that can be configured as an HTTPS server, a proxy server, and a virtual-host server.

Affected versions of this package are vulnerable to Improper Input Validation. WEBrick lets attackers to inject malicious escape sequences to its logs, making it possible for dangerous control characters to be executed on a victim's terminal emulator. This is due to data being written to a log file without sanitizing non-printable characters. Remote attackers could modify a window's title, execute arbitrary commands, or overwrite files via an HTTP request containing an escape sequence for a terminal emulator.

## PoC

```
% 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
```

## References

- [RedHat Bugzilla Bug](#)
- [Ruby-Lang News](#)
- [Security Focus](#)
- [Security Tracker](#)

## CVSS Base Scores

version 3.1

▼ Snyk		9.8 CRITICAL			
Attack Vector (AV)	Network	Scope (S)	Unchanged	Confidentiality (C)	High
Attack Complexity (AC)	Low			Integrity (I)	High
Privileges Required (PR)	None			Availability (A)	High
User Interaction (UI)	None				
> NVD		5.3 MEDIUM			

## Severity

RECOMMENDED



CVSS assessment by Snyk's Security Team. [Learn more](#)

## Threat Intelligence

Exploit Maturity

PROOF OF CONCEPT

EPSS

18.65% (95<sup>th</sup> percentile)

## Do your applications use this vulnerable package?

In a few clicks we can analyze your entire application and see what components are vulnerable in your application, and suggest you quick fixes.

Test your applications

## Snyk Learn

Learn about Improper Input Validation vulnerabilities in an interactive lesson.

Start learning

Snyk ID SNYK-RUBY-WEBRICK-1315609

Published 1 Jul 2021

Disclosed 1 Jul 2021

Credit Giovanni Pellerano (@evilaliv3), Alessandro Tanasi (@jekil), Francesco Ongaro (@ascii)

[Report a new vulnerability](#)

[Found a mistake?](#)

#### PRODUCT

[Snyk Open Source](#)  
[Snyk Code](#)  
[Snyk Container](#)  
[Snyk Infrastructure as Code](#)  
[Snyk AppRisk](#)

#### RESOURCES

[Vulnerability DB](#)  
[Documentation](#)  
[Disclosed Vulnerabilities](#)  
[Blog](#)  
[FAQs](#)

#### COMPANY

[About](#)  
[Jobs](#)  
[Contact](#)  
[Policies](#)  
[Do Not Sell My Personal Information](#)

#### CONTACT US

[Support](#)  
[Report a new vuln](#)  
[Events](#)

#### FIND US ONLINE



#### TRACK OUR DEVELOPMENT



© 2025 Snyk Limited

Registered in England and Wales. Company number: 09677925

Registered address: Highlands House, Basingstoke Road, Spencers Wood, Reading, Berkshire, RG7 1NT.