PRESS REVIEW ARCHIVE

Digital Media Monitoring & Documentation Service

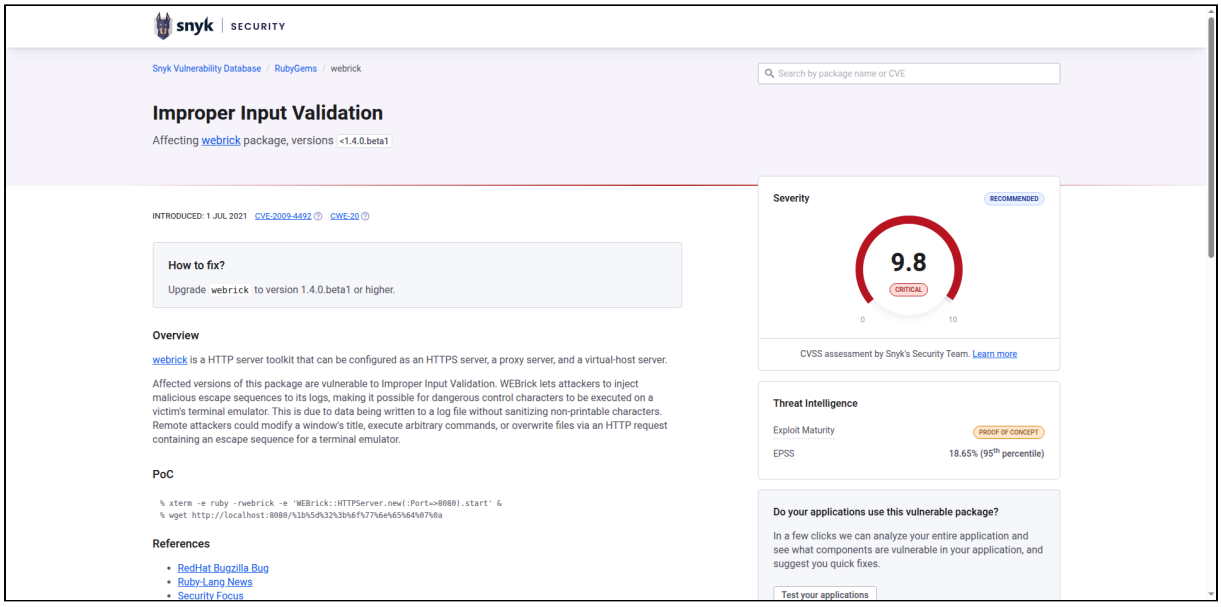
Source URL: https://security.snyk.io/vuln/SNYK-RUBY-WEBRICK-1315609

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

Page Screenshot



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% (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

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?