



## Task3\_NessusScan

---

Report generated by Tenable Nessus™

Mon, 17 Nov 2025 17:25:32 IST

---

---

## TABLE OF CONTENTS

---

### Vulnerabilities by Host

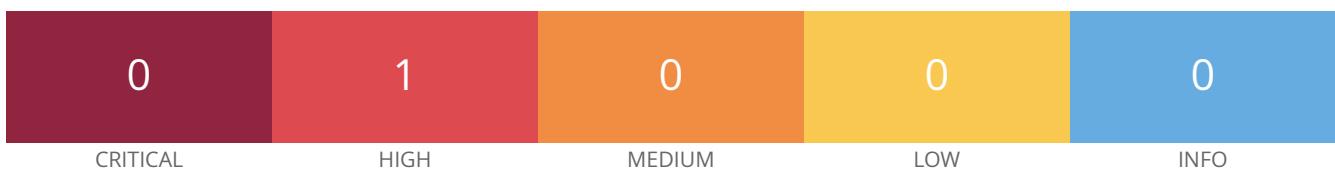
- 127.0.0.1.....4

---

## Vulnerabilities by Host

---

# 127.0.0.1



## Host Information

IP: 127.0.0.1

## Vulnerabilities

**270698 - Ruby RACK < 2.2.20 / 3.x < 3.1.18 / 3.2 < 3.2.3 Multiple Vulnerabilities**

## Synopsis

The remote host has an application installed that is affected by DoS vulnerability.

## Description

The version of the RACK Ruby library installed on the remote host is prior to 2.2.20 / 3.1.18 / 3.2.3. It is, therefore, affected by the following vulnerabilities:

- Rack::Request#POST reads the entire request body into memory for Content-Type: application/x-www-form-urlencoded, calling rack.input.read(nil) without enforcing a length or cap. Large request bodies can therefore be buffered completely into process memory before parsing, leading to denial of service (DoS) through memory exhaustion. (CVE-2025-61919)
- A possible information disclosure vulnerability existed in Rack::Sendfile when running behind a proxy that supports x-sendfile headers (such as Nginx). Specially crafted headers could cause Rack::Sendfile to miscommunicate with the proxy and trigger unintended internal requests, potentially bypassing proxy-level access restrictions. (CVE-2025-61780)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

## See Also

<https://github.com/rack/rack/security/advisories/GHSA-r657-rxjc-j557>

<https://github.com/rack/rack/security/advisories/GHSA-6xw4-3v39-52mm>

## Solution

Upgrade to RACK version 2.2.20 / 3.1.18 / 3.2.3 or later.

## Risk Factor

High

#### CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

#### VPR Score

4.4

#### EPSS Score

0.0062

#### CVSS v2.0 Base Score

7.8 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:C)

#### STIG Severity

I

#### References

CVE                  CVE-2025-46727  
CVE                  CVE-2025-61919  
XREF                IAVB:2025-B-0171

#### Plugin Information

Published: 2025/10/17, Modified: 2025/10/17

#### Plugin Output

tcp/0

```
Path : /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/rack-3.1.16
Installed version : 3.1.16
Fixed version : 3.1.18
```