NVD

VULNERABILITIES

CVE-2025-61780 Detail

Description

Rack is a modular Ruby web server interface. Prior to versions 2.2.20, 3.1.18, and 3.2.3, 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. When `Rack::Sendfile` received untrusted `x-sendfile-type` or `x-accel-mapping` headers from a client, it would interpret them as proxy configuration directives. This could cause the middleware to send a "redirect" response to the proxy, prompting it to reissue a new internal request that was not subject to the proxy's access controls. An attacker could exploit this by setting a crafted `x-sendfile-type: x-accel-redirect` header, setting a crafted `x-accel-mapping` header, and requesting a path that qualifies for proxy-based acceleration. Attackers could bypass proxy-enforced restrictions and access internal endpoints intended to be protected (such as administrative pages). The vulnerability did not allow arbitrary file reads but could expose sensitive application routes. This issue only affected systems meeting all of the following conditions: The application used `Rack::Sendfile` with a proxy that supports `x-accel-redirect` (e.g., Nginx); the proxy did **not** always set or remove the `x-sendfile-type` and `x-accel-mapping` headers; and the application exposed an endpoint that returned a body responding to `.to_path`. Users should upgrade to Rack versions 2.2.20, 3.1.18, or 3.2.3, which require explicit configuration to enable `x-accel-redirect`. Alternatively, configure the proxy to always set or strip the header, or in Rails applications, disable sendfile completely.

Metrics

CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

NIST: NVD
Base Score: 5.3 MEDIUM
Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CNA: GitHub, Inc.
Base Score: 5.8 MEDIUM
Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

URL	Source(s)	Tag(s)
https://github.com/rack/rack/commit/57277b7741581fa827472c5c666f6e6a33abd784	GitHub, Inc.	**Patch**
https://github.com/rack/rack/commit/7e69f65eefe9cd2868df9f9f3b0977b86f93523a	GitHub, Inc.	**Patch**
https://github.com/rack/rack/commit/fba2c8bc63eb787ff4b19bc612d315fda6126d85	GitHub, Inc.	**Patch**
https://github.com/rack/rack/security/advisories/GHSA-r657-rxjc-j557	GitHub, Inc.	**Mitigation** **Vendor Advisory**

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor	GitHub, Inc.
CWE-441	Unintended Proxy or Intermediary ('Confused Deputy')	GitHub, Inc.
CWE-913	Improper Control of Dynamically-Managed Code Resources	GitHub, Inc.

Known Affected Software Configurations Switch to CPE 2.2

Configuration 1 (hide)

cpe:2.3:a:rack:rack:*:*:*:*:*:ruby:*:* Show Matching CPE(s)	**Up to (excluding)** **2.2.20**	
cpe:2.3:a:rack:rack:*:*:*:*:*:ruby:*:* Show Matching CPE(s)	**From (including)** **3.0.0**	**Up to (excluding)** **3.1.18**
cpe:2.3:a:rack:rack:*:*:*:*:*:ruby:*:* Show Matching CPE(s)	**From (including)** **3.2.0**	**Up to (excluding)** **3.2.3**

Denotes Vulnerable Software

Are we missing a CPE here? Please let us know.

Change History

2 change records found show changes

QUICK INFO

CVE Dictionary Entry:
CVE-2025-61780

NVD Published Date:
10/10/2025

NVD Last Modified:
10/30/2025

Source:
GitHub, Inc.

HEADQUARTERS
100 Bureau Drive
Gaithersburg, MD 20899
(301) 975-2000

Incident Response Assistance and Non-NVD Related Technical Cyber Security Questions:
US-CERT Security Operations Center
Email: soc@us-cert.gov
Phone: 1-888-282-0870