MCP Ruby SDK: Insufficient Session Binding Allows SSE Stream Hijacking via Session ID Replay

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-33946
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-27 22:16:21 UTC
Updated	2026-04-02 15:23:21 UTC
Description	MCP Ruby SDK is the official Ruby SDK for Model Context Protocol servers and clients. Prior to version 0.9.2, the Ruby SD

Risk And Classification

Primary CVSS: v4.0 8.2 HIGH from security-advisories@github.com

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000480000 probability, percentile 0.148060000 (date 2026-04-01)

Problem Types: CWE-384 | CWE-639 | CWE-384 CWE-384: Session Fixation | CWE-639 CWE-639: Authorization Bypass Through User-Controlled Key

Version	Source	Type	Score	Severity	Vector
4.0	security-advisories@github.com	Secondary	8.2	HIGH	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/S
4.0	CNA	DECLARED	8.2	HIGH	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/S
3.1	nvd@nist.gov	Primary	5.9	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

None

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

None

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Lfprojects	Mcp Ruby Sdk	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms

CNA	Modelcontextprotocol	Ruby-sdk	affected < 0.9.2	Not specified

References

Reference	Source	Link
github.com/modelcontextprotocol/python-sdk/blob/main/src/mcp/server/stre...	security-advisories@github.com	github.com
github.com/modelcontextprotocol/ruby-sdk/blob/main/examples/streamable_h...	security-advisories@github.com	github.com
github.com/modelcontextprotocol/go-sdk/blob/main/mcp/streamable.go	security-advisories@github.com	github.com
github.com/modelcontextprotocol/csharp-sdk/blob/main/src/ModelContextPro...	security-advisories@github.com	github.com
github.com/modelcontextprotocol/ruby-sdk/commit/db40143402d65b4fb6923cec...	security-advisories@github.com	github.com
github.com/modelcontextprotocol/ruby-sdk/releases/tag/v0.9.2	security-advisories@github.com	github.com
github.com/modelcontextprotocol/ruby-sdk/security/advisories/GHSA-qvqr-5...	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com
hackerone.com/reports/3556146	security-advisories@github.com	hackerone.c
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.