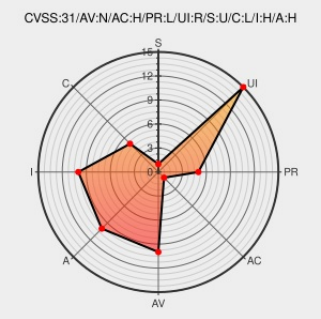
CVE-2021-21368

Published on: 03/12/2021 12:00:00 AM UTC

Last Modified on: 10/24/2022 05:11:00 PM UTC

CVE-2021-21368 - advisory for GHSA-gmjw-49p4-pcfm

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Msgpack5 from Msgpack5 Project contain the following vulnerability:

msgpack5 is a msgpack v5 implementation for node.js and the browser. In msgpack5 before versions 3.6.1, 4.5.1, and 5.2.1 there is a "Prototype Poisoning" vulnerability. When msgpack5 decodes a map containing a key "__proto__", it assigns the decoded value to __proto__. Object.prototype.__proto__ is an accessor property for the receiver's prototype. If the value corresponding to the key __proto__ decodes to an object or null, msgpack5 sets the decoded object's prototype to that value. An attacker who can submit crafted MessagePack data to a service can use this to produce values that appear to be of other types; may have unexpected prototype properties and methods (for example length, numeric properties, and push et al if __proto__'s value decodes to an Array); and/or may throw unexpected exceptions when used (for example if the __proto__ value decodes to a Map or Date). Other unexpected behavior might be produced for other types. There is no effect on the global prototype. This "prototype poisoning" is sort of a very limited inversion of a prototype pollution attack. Only the decoded value's prototype is affected, and it can only be set to msgpack5 values (though if the victim makes use of custom codecs, anything could be a msgpack5 value). We have not found a way to escalate this to true prototype pollution (absent other bugs in the consumer's code). This has been fixed in msgpack5 version 3.6.1, 4.5.1, and 5.2.1. See the referenced GitHub Security Advisory for an example and more details.

CVE-2021-21368 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **mcollina** - **msgpack5** version **< 3.6.1**

Affected Vendor/Software: **mcollina** - **msgpack5** version **>= 4.0.0, < 4.5.1**

Affected Vendor/Software: **mcollina** - **msgpack5** version **>= 5.0.0, < 5.2.1**

CVSS3 Score: 8.8 - HIGH

Attack	Attack	Privileges	User

Vector	Complexity	Required	Interaction
NETWORK	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Merge pull request from GHSA-gmjw-49p4-pcfm · mcollina/msgpack5@d4e6cb9 · GitHub	Patch, Third Party Advisory, github.com, text/html	MISC github.com/mcollina/msgpack5/commit/d4e6cb956ae51c8bb2828e71c7c1107c340cf1e
Release v4.5.1 · mcollina/msgpack5 · GitHub	Release Notes, Third Party Advisory, github.com, text/html	MISC github.com/mcollina/msgpack5/releases/tag/v4.5.1
msgpack5	Product, Third Party Advisory, www.npmjs.com, text/html	MISC www.npmjs.com/package/msgpack5
Release v3.6.1 · mcollina/msgpack5 · GitHub	Release Notes, Third Party Advisory, github.com, text/html	MISC github.com/mcollina/msgpack5/releases/tag/v3.6.1
Release v5.2.1 · mcollina/msgpack5 · GitHub	Release Notes, Third Party Advisory, github.com, text/html	MISC github.com/mcollina/msgpack5/releases/tag/v5.2.1
Prototype poisoning · Advisory · mcollina/msgpack5 · GitHub	Exploit, Third Party Advisory, github.com, text/html	CONFIRM github.com/mcollina/msgpack5/security/advisories/GHSA-gmjw-49p4-pcfm

Related QID Numbers

982906 Nodejs (npm) Security Update for msgpack5 (GHSA-gmjw-49p4-pcfm)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Msgpack5 Project	Msgpack5	All	All	All	All

cpe:2.3:a:msgpack5_project:msgpack5:*:*:*:*:*:node.js:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→