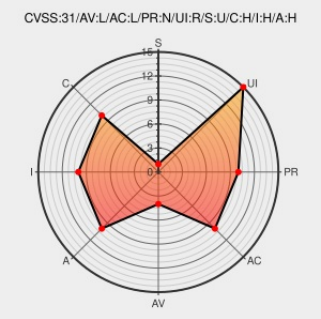
CVE-2020-24807

Published on: 10/06/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:38 PM UTC

CVE-2020-24807

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



Certain versions of Socket.io-file from Socket.io-file Project contain the following vulnerability:

** UNSUPPORTED WHEN ASSIGNED ** The socket.io-file package through 2.0.31 for Node.js relies on client-side validation of file types, which allows remote attackers to execute arbitrary code by uploading an executable file via a modified JSON name field. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.

CVE-2020-24807 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
socket.io-file - npm	Product Third Party Advisory	MISC www.npmjs.com/package/socket.io-

	www.npmjs.com text/html	file
GitHub - rico345100/socket.io-file: Socket.io-file is a node module for uploading file via Socket.io module	Product Third Party Advisory github.com text/html	MISC github.com/rico345100/socket.io-file
Overview	Third Party Advisory www.npmjs.com text/html	MISC www.npmjs.com/advisories/1564
File restriction bypass in socket.io-file · GHSA-6495-8jvh-f28x · GitHub Advisory Database · GitHub	Third Party Advisory github.com text/html	MISC github.com/advisories/GHSA-6495-8jvh-f28x

Related QID Numbers

982623 Nodejs (npm) Security Update for socket.io-file (GHSA-r2gr-fhmr-66c5)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Socket.io-file Project	Socket.io-file	All	All	All	All

cpe:2.3:a:socket.io-file_project:socket.io-file:*:*:*:*:*:node.js:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@PenTestMag	[CVE-2020-24807] File Type Restriction Bypass in Socket.io-file NPM module pentestmag.com/cve-2020-24807… #pentest… twitter.com/i/web/status/1…	2021-05-30 22:34:21
@Anastasis_King	[CVE-2020-24807] File Type Restriction Bypass in Socket.io-file NPM module pentestmag.com/cve-2020-24807… #pentest… twitter.com/i/web/status/1…	2021-05-31 10:24:44
@PenTestMag	[CVE-2020-24807] File Type Restriction Bypass in Socket.io-file NPM module pentestmag.com/cve-2020-24807… #pentest… twitter.com/i/web/status/1…	2021-08-09 15:20:43
@PenTestMag	[CVE-2020-24807] File Type Restriction Bypass in Socket.io-file NPM module pentestmag.com/cve-2020-24807… #pentest… twitter.com/i/web/status/1…	2021-08-16 18:37:03
@PenTestMag	[CVE-2020-24807] File Type Restriction Bypass in Socket.io-file NPM module pentestmag.com/cve-2020-24807… #pentest… twitter.com/i/web/status/1…	2021-09-10 12:10:13
@PenTestMag	[CVE-2020-24807] File Type Restriction Bypass in Socket.io-file NPM module pentestmag.com/cve-2020-24807… #pentest… twitter.com/i/web/status/1…	2021-10-18 12:13:32
@PenTestMag	[CVE-2020-24807] File Type Restriction Bypass in Socket.io-file NPM module pentestmag.com/cve-2020-24807… #pentest… twitter.com/i/web/status/1…	2021-11-04 16:28:30
@PenTestMag	[CVE-2020-24807] File Type Restriction Bypass in Socket.io-file NPM module pentestmag.com/cve-	2021-11-19

@PenTestMag	2020-24807… #pentest… twitter.com/i/web/status/1…	00:25:07
@PenTestMag	[CVE-2020-24807] File Type Restriction Bypass in Socket.io-file NPM module pentestmag.com/cve-2020-24807… #pentest… twitter.com/i/web/status/1…	2021-12-08 19:34:19
@PenTestMag	[CVE-2020-24807] File Type Restriction Bypass in Socket.io-file NPM module pentestmag.com/cve-2020-24807… #pentest… twitter.com/i/web/status/1…	2021-12-15 18:12:42
@PenTestMag	[CVE-2020-24807] File Type Restriction Bypass in Socket.io-file NPM module pentestmag.com/cve-2020-24807… #pentest… twitter.com/i/web/status/1…	2022-02-08 13:49:30
@PenTestMag	[CVE-2020-24807] File Type Restriction Bypass in Socket.io-file NPM module pentestmag.com/cve-2020-24807… #pentest… twitter.com/i/web/status/1…	2022-04-21 21:53:06
@PenTestMag	[CVE-2020-24807] File Type Restriction Bypass in Socket.io-file NPM module pentestmag.com/cve-2020-24807… #pentest… twitter.com/i/web/status/1…	2022-06-07 12:07:14
@PenTestMag	[CVE-2020-24807] File Type Restriction Bypass in Socket.io-file NPM module pentestmag.com/cve-2020-24807… #pentest… twitter.com/i/web/status/1…	2022-07-05 15:50:12
@PenTestMag	[CVE-2020-24807] File Type Restriction Bypass in Socket.io-file NPM module pentestmag.com/cve-2020-24807… #pentest… twitter.com/i/web/status/1…	2022-08-18 16:06:05
@PenTestMag	[CVE-2020-24807] File Type Restriction Bypass in Socket.io-file NPM module pentestmag.com/cve-2020-24807… #pentest… twitter.com/i/web/status/1…	2022-09-12 18:43:00

← Previous ID

Next ID→