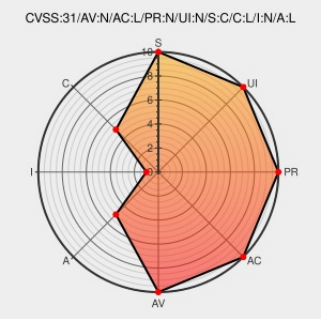
CVE-2020-12827

Published on: 06/17/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:35 PM UTC

CVE-2020-12827

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



Certain versions of Mjml from Mjml contain the following vulnerability:

MJML prior to 4.6.3 contains a path traversal vulnerability when processing the mj-include directive within an MJML document.

CVE-2020-12827 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.2 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	LOW	NONE	LOW

CVSS2 Score: 6.4 - MEDIUM

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

CVE References

Description	Tags	Link
RCE Security – Remote Code Execution Techniques and more	Broken Link, rcesecurity.com, text/html	MISC rcesecurity.com
Release v4.6.3 · mjmlio/mjml	Release Notes	MISC github.com/mjmlio/mjml/releases/tag/v4.6.3

· GitHub	Third Party Advisory github.com text/html	
expose ignoreIncludes on mjml2html · mjmlio/mjml@30e29ed · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/mjmlio/mjml/commit/30e29ed2cdaec8684d60a6d12ea07b611c765a12
Full Disclosure: [CVE-2020-12827] MJML <= 4.6.2 mj-include "path" Path Traversal	Exploit Mailing List Third Party Advisory seclists.org text/html	FULLDISC 20200616 [CVE-2020-12827] MJML <= 4.6.2 mj-include "path" Path Traversal
MJML 4.6.2 Path Traversal ≈ Packet Storm	Exploit Third Party Advisory VDB Entry packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/158111/MJML-4.6.2-Path-Traversal.html
Community - MJML	Vendor Advisory mjml.io text/html	MISC mjml.io/community
mjml. (@mjmlio) | Twitter	Third Party Advisory nitter.domain.glass text/html	MISC twitter.com/mjmlio

Related QID Numbers

995651 NodeJs (Npm) Security Update for mjml (GHSA-4hch-r9xf-6vfr)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mjml	Mjml	All	All	All	All
Application	Mjml	Mjml	All	All	All	All

cpe:2.3:a:mjml:mjml:*:*:*:*:*:*:*:*:

cpe:2.3:a:mjml:mjml:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report