[CVE-2020-12827] MJML <= 4.6.2 mj-include "path" Path Traversal

From: "Julien Ahrens (RCE Security)" <info () rcesecurity com>
Date: Sun, 14 Jun 2020 13:15:49 +0000

```
RCE Security Advisory
https://www.rcesecurity.com


1. ADVISORY INFORMATION
=======================
Product:         MJML
Vendor URL:      https://github.com/mjmlio/mjml/
Type:            Path Traversal [CWE-22]
Date found:      2020-04-28
Date published:  2020-06-14
CVSSv3 Score:    7.2 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:L)
CVE:             CVE-2020-12827


2. CREDITS
==========
This vulnerability was discovered and researched by Julien Ahrens from
RCE Security.


3. VERSIONS AFFECTED
====================
MJML <= 4.6.2

As a solution MJML disabled mj-include by default in MJML v4.6.3 by adding the
"ignoreIncludes" directive, however, the component could still be explicitly
enabled, making the application vulnerable again.


4. INTRODUCTION
===============
MJML is a markup language created by Mailjet and designed to reduce the pain of
coding a responsive email. Its semantic syntax makes it easy and straightforward
while its rich standard components library fastens your development time and
lightens your email codebase. MJML's open-source engine takes care of
translating the MJML you wrote into responsive HTML.

(from the vendor's homepage)


5. VULNERABILITY DETAILS
========================
MJML offers a component called "mj-include" that allows other external MJML
files to be included into the email template by using its "path" attribute.
(see https://mjml.io/documentation/#mj-include).

However MJML does not properly validate the value supplied to the "path"
argument, allowing an attacker to traverse directories or even directly point to
other system files outside of the web server's root directory.

However since MJML expects the referenced file to be in the format of a MJML
file, the attack scope is limited to:

- Leaking the local server path by pointing to a non-existing MJML file, which
throws an error containing the full path, i.e.:
<mjml><mj-include path='test'/></mjml>

- Enumerating local server files by using a true/false approach. Existing server
files return an error, while non-existing do not:
<mjml><mj-include path='/etc/passwd'/></mjml>

- Partially reading local binary server files. Pointing path to binary files
throws an error, but the error message does contain a portion of the referenced
file. On this way it is possible to leak parts of i.e. compressed local log
files:
<mjml><mj-include path='/var/log/apt/history.log.1.gz'/></mjml>

- Causing denial of service conditions on the application embedding MJML, by
reading i.e. /dev/urandom:
<mjml><mj-include path='/dev/urandom'/></mjml>


6. RISK
=======
The vulnerability can be used by an unauthenticated attacker or authenticated
attacker depending on how MJML is embedded to leak sensitive information about
the server such as local server paths and contents of compressed/binary files
or cause denial of service attacks against the application.


7. SOLUTION
===========
Update MJML to version 4.6.3 and keep "ignoreIncludes" set to false.


8. REPORT TIMELINE
==================
2020-04-28: Discovery of the vulnerability
2020-04-30: Reported the vulnerability to maintainers of MJML
2020-05-05: MJML pushes a fix disabling includes by default.
2020-05-11: CVE requested from MITRE
2020-05-13: MITRE assigns CVE-2020-12827
2020-06-14: Public disclosure.


9. REFERENCES
=============
https://github.com/mjmlio/mjml/commit/30e29ed2cdaec8684d60a6d12ea07b611c765a12


_______________________________________________
Sent through the Full Disclosure mailing list
https://nmap.org/mailman/listinfo/fulldisclosure
Web Archives & RSS: http://seclists.org/fulldisclosure/
```

[CVE-2020-12827] MJML <= 4.6.2 mj-include "path" Path Traversal ***Julien Ahrens (RCE Security) (Jun 16)***