MJML 4.6.2 Path Traversal

Authored by Julien Ahrens | Site rcesecurity.com

Posted Jun 16, 2020

MJML versions 4.6.2 and below suffer from a path traversal vulnerability.

tags | exploit, file inclusion
advisories | CVE-2020-12827
SHA-256 | 166961aa7a1aa4863ba6a1c75fcc9e0116bd4fd9789c3759ca27ecb57c656da5 **Download | Favorite | View**

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
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
```

Login or Register to add favorites

Follow us on Twitter

Subscribe to an RSS Feed

File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr
Sa					
				1	2
3					
4	5	6	7	8	9
10					
11	12	13	14	15	16
17					
18	19	20	21	22	23
24					
25	26	27	28	29	30
31					

Top Authors In Last 30 Days

Red Hat 154 files
Ubuntu 73 files
LiquidWorm 23 files
Debian 18 files
malvuln 11 files
nu11secur1ty 11 files
Gentoo 9 files
Google Security Research 8 files
T. Weber 4 files
Julien Ahrens 4 files

File Tags

ActiveX (932)
Advisory (79,754)
Arbitrary (15,694)
BBS (2,859)
Bypass (1,619)
CGI (1,018)
Code Execution (6,926)
Conference (673)
Cracker (840)
CSRF (3,290)
DoS (22,602)
Encryption (2,349)
Exploit (50,359)
File Inclusion (4,165)
File Upload (946)
Firewall (821)
Info Disclosure (2,660)
Intrusion Detection (867)
Java (2,899)
JavaScript (821)
Kernel (6,291)
Local (14,201)
Magazine (586)
Overflow (12,419)
Perl (1,418)
PHP (5,093)
Proof of Concept (2,291)
Protocol (3,435)
Python (1,467)
Remote (30,044)
Root (3,504)
Ruby (594)
Scanner (1,631)
Security Tool (7,777)
Shell (3,103)
Shellcode (1,204)
Sniffer (886)

File Archives

December 2022
November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
Older

Systems

AIX (426)
Apple (1,926)
BSD (370)
CentOS (55)
Cisco (1,917)
Debian (6,634)
Fedora (1,690)
FreeBSD (1,242)
Gentoo (4,272)
HPUX (878)
iOS (330)
iPhone (108)
IRIX (220)
Juniper (67)
Linux (44,315)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,469)
Slackware (941)
Solaris (1,607)

Spoof (2,166)
SQL Injection (16,102)
TCP (2,379)
Trojan (686)
UDP (876)
Virus (662)
Vulnerability (31,136)
Web (9,365)
Whitepaper (3,729)
x86 (946)
XSS (17,494)
Other

SUSE (1,444)
Ubuntu (8,199)
UNIX (9,159)
UnixWare (185)
Windows (6,511)
Other

packet storm

Site Links
- News by Month
- News Tags
- Files by Month
- File Tags
- File Directory

About Us
- History & Purpose
- Contact Information
- Terms of Service
- Privacy Statement
- Copyright Information

Hosting By
- Rokasec

Follow us on Twitter

Subscribe to an RSS Feed