Press This CSRF DoS

Cross-Site Request Forgery (CSRF) is a type of attack that causes an action to be unintentionally performed after a user has clicked a link or submitted some type of form, which would then automatically execute the attack. The founder of the exploit, Sipke Mellema, mentioned that this exploit was found during a “Summer of Pwnage” event where hackers gather to find vulnerabilities in open-source software such as WordPress. Mellema discovered that this exploit could be used to create a Denial of Service (DoS) upon opening a bad URL from within the Press This page. He mentions that Press This can execute a function that will scan a URL for content; and by using a GET request to “/wp-admin/press-this.php?***u=<URL>***&url-scan-submit=Scan”, the page will download all contents from the external server where “**<URL>**” is placed. And since there is no limit to the amount of content that could be downloaded, attackers can set the URL to scan and download a large file from an external server, which could use up processing power to process the large data. He mentions that the URL can be called multiple times rendering the word press server to be inaccessible. Mellema did not explain how the exploit was fixed.

References

<https://hackerone.com/reports/153093>

<https://sumofpwn.nl/advisory/2016/cross_site_request_forgery_in_wordpress_press_this_function_allows_dos.html>