Topher Tebow

June 7, 2022

Cross-Site Scripting Vulnerability In Download Manager Plugin

On May 30, 2022, Security Researcher Rafie Muhammad reported a reflected Cross-Site Scripting (XSS) vulnerabilit us that they discovered in Download Manager, a WordPress plugin installed on over 100,000 sites. On request, we assigned a vulnerability identifier of CVE-2022-1985.

All Wordfence users, including Free, Premium, Care, and Response, are protected from exploits targeting this vulnerability thanks to the Wordfence Firewall's built-in Cross-Site Scripting protection.

Even though Wordfence provides protection against this vulnerability, we strongly recommend ensuring that your s has been updated to the latest patched version of Download Manager, which is version 3.2.43 at the time of this publication.

Description: Reflected Cross-Site Scripting
Affected Plugin: Download Manager
Plugin Slug: download-manager
Plugin Developer: codename065
Affected Versions: <= 3.2.42
CVE ID: CVE-2022-1985
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: Rafie Muhammad (Yeraisci)
Fully Patched Version: 3.2.43

Download Manager is a file and document management plugin to help manage and control file downloads with

vulnerable to reflected Cross-Site Scripting.Secure coding practices would include checks to sanitize the input received by the page, and escaping that code on the output to ensure that only approved inputs and outputs are presented. Unfortunately, insufficient input sanitization and output escaping on the `$_REQUEST['frameid']` parame found in the `~/src/Package/views/shortcode-iframe.php` file of the Download Manager plugin made it possible an attacker to run arbitrary code in a victim's browser by getting them to click on a specially crafted URL. This is because the '`frameid`' parameter was echoed to the page without sufficient user input validation.

```
219         //window.parent.document.wpdm_adjust_frame_height("<?php echo $_REQUEST['frameid']; ?>",
$(document).height());
220         //window.parent.document.getElementById("<?php echo $_REQUEST['frameid']; ?>").style.height
$(document).height()+"px";
221         //window.parent.document.getElementById("<?php echo $_REQUEST['frameid']; ?>").height =
$(document).height()+"px";
```

Without proper sanitization and escaping in place on user-supplied inputs, JavaScript can be used to manipulate th page. Even an unsophisticated attacker could hijack the form and use it to trick a site administrator into unknowing disclosing sensitive information, or to collect cookie values.

More specialized attackers would use this capability to gain administrator access or add a backdoor and take over site. If the attacker gains this access, they would have access to the same information the administrator would be able to access, including user details and customer information.

In the case of Download Manager, customer information and access to digital products would both be at risk. If an attacker were able to trick an administrator into clicking a link that has been designed to send session cookies to tl attacker, add a malicious administrator account, or implement a backdoor on the website, the attacker would also have free reign in the administrator panel, giving them the ability to modify checkout settings and even add fake products to the website.

Conclusion

In today's post, we discussed a reflected Cross-Site Scripting (XSS) vulnerability in Download Manager. While this would require tricking an administrator into clicking a link or performing some other action, it still offers the potenti for site takeover. As such we urge you to update to the latest version of this plugin, 3.2.43 as of this writing, as soo as possible.

All Wordfence users, including Free, Premium, Care, and Response, are protected from exploits targeting this vulnerability.

If you believe your site has been compromised as a result of this vulnerability or any other vulnerability, we offer Incident Response services via Wordfence Care. If you need your site cleaned immediately, Wordfence Response offers the same service with 24/7/365 availability and a 1-hour response time. Both these products include hands- support in case you need further assistance.

If you know a friend or colleague who is using this plugin on their site, we highly recommend forwarding this advisc to them to help keep their sites protected, as this is a serious vulnerability that can lead to complete site takeover.

Congratulations to Ravie Muhammad for discovering and responsibly disclosing this vulnerability to the plugin's developers. As a reminder, Wordfence is a CVE Numbering Authority (CNA) and we can assign CVE IDs to your vulnerability discoveries in WordPress Plugins, Themes, and Core. If you need a CVE for one of your WordPress finc please fill out our form here. Your vulnerability discovery may be featured on our blog with your permission!

Comments

3 Comments

Kevin *
June 8, 2022

When I click Shaon it takes me to a Pro website, but when I click 'view details' it takes me to the W3 Eden plugin details which are the same as this post relates to.

Does anyone have any ideas why my version is later than the latest version of the plugin? The latest version is 3.2.43 according to th details page.

I do have Wordfence installed on this website, so wondering if I need to worry or not. I'd prefer to take make sure I am running the latest version and fully protected but I can't update as it says I'm on a newer version. Very weird.

Any help would be greatly appreciated =)

Chloe Chamberland *
June 8, 2022
4:31 am

Hi Kevin!

For starters you can rest assured knowing the Wordfence firewall has your site covered - any exploits attempting to target this vulnerability will be blocked by the firewall's built-in Cross-Site Scripting protection. The PRO version of the Download Manager plugin appears to have been patched in version 6.1.7. I did some research and it looks like Donwnload Manager used to be maintained by Shaon so you likely have an older copy of the plugin running on your site. I recommend reaching out to their support team to assist you in updating to the latest version of the free plugin (3.2.43) or the pro version (6.1.7) depending on what your site is running.

I hope that helps!

GOBINDA TARAFDAR *
June 8, 2022
10:25 pm

Hi Kevin,
Most probably Shaon is another name of the plugin author Shahjada. Check his plugin author page, his wp org slack name is @shac
https://profiles.wordpress.org/codename065/#content-plugins
If you are using their pro addons then you will see the name. Also, find the same thing in the comment section on this page - wpdownloadmanager .com /download/advanced-custom-fields/
Thanks.

Wordfence Free
Wordfence Premium
Wordfence Care
Wordfence Response
Wordfence Central

Documentation
Learning Center
Free Support
Premium Support

Blog
In The News
Vulnerability Advisories

About Wordfence
Careers
Contact
Security
CVE Request Form

Stay Updated

Sign up for news and updates from our panel of experienced security professionals.

you@example.com

By checking this box I agree to the terms of service and privacy policy.*

SIGN UP