DOM XSS in microweber ver 1.2.15 in microweber/microweber

0

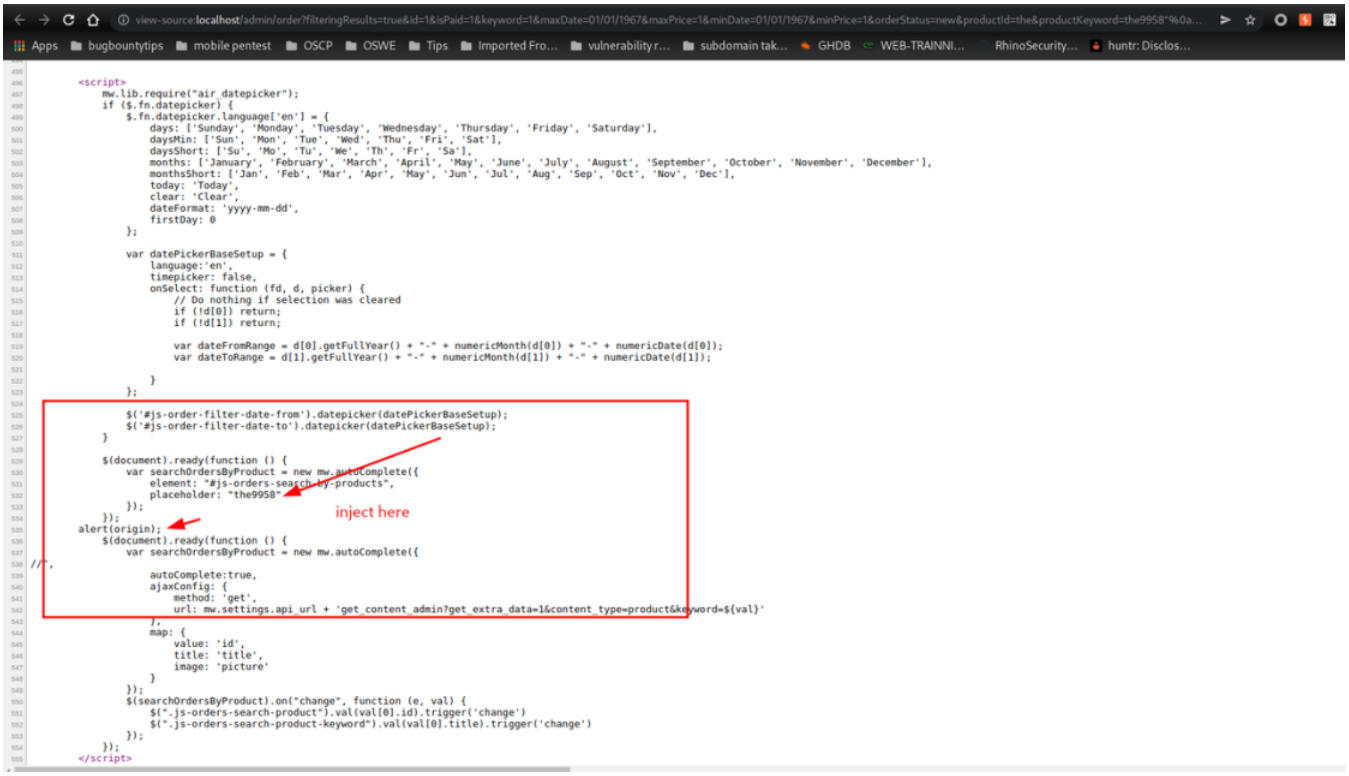
Valid Reported on Apr 28th 2022

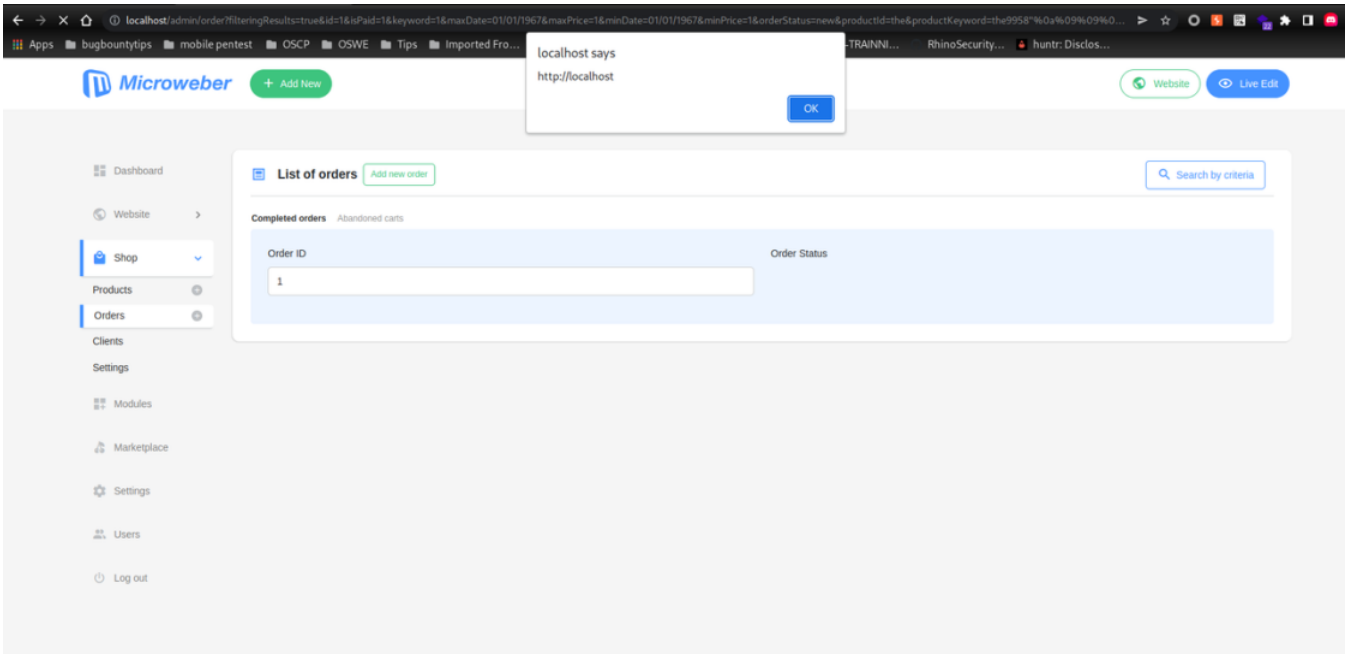
Description

Hi there, on your latest version docker images 3463db62a01f, vulnerable to DOM XSS.

Proof of Concept

```
http://localhost/admin/order?filteringResults=true&id=1&isPaid=1&keyword=1&
```





Impact

inject arbitrary js code, deface website, steal cookie...

Occurrences

order_filtering.blade.php L157

DOM code

```
$(document).ready(function () {
                var searchOrdersByProduct = new mw.autoComplete({
                    element: "#js-orders-search-by-products",
                    placeholder: "<?php if ($productKeyword) { echo $pr
                    autoComplete:true,
                    ajaxConfig: {
                        method: 'get',
                        url: mw.settings.api_url + 'get_content_admin?g
                    },
                    map: {
                        value: 'id',
                        title: 'title',
                        image: 'picture'
```

```
                    image: "picture"
                }
            });
            $(searchOrdersByProduct).on("change", function (e, val)
                $(".js-orders-search-product").val(val[0].id).trigg
                $(".js-orders-search-product-keyword").val(val[0].t
            });
        });
```

CVE
CVE-2022-1555
(Published)

Vulnerability Type
CWE-79: Cross-site Scripting (XSS) - DOM

Severity
High (8.8)

Registry
Other

Affected Version
1.2.15

Visibility
Public

Status
Fixed

Found by

Minh
@minhnb11
pro

Fixed by

Bozhidar Slaveykov
@bobimicroweber
maintainer

maintainer

This report was seen 679 times.

We are processing your report and will contact the **microweber** team within 24 hours. 7 months ago

We have contacted a member of the **microweber** team and are waiting to hear back 7 months ago

We have sent a follow up to the **microweber** team. We will try again in 7 days. 7 months ago

Bozhidar Slaveykov validated this vulnerability 7 months ago

Minh has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Jamie Slome 7 months ago — Admin

@bobimicroweber - I can see you hit a bit of an error here, would you like me to update the CVSS for you?

Bozhidar Slaveykov marked this as fixed in **1.2.16** with commit **724e2d** 7 months ago

Bozhidar Slaveykov has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

order_filtering.blade.php#L157 has been validated ✔

Bozhidar 7 months ago

The UI of the huntr is changed and i can't see where is the severity... Can you turn back old design of the huntr? The severity of this issue is low. Yes you can change it for me

Jamie Slome 7 months ago — Admin

@bobimicroweber - if possible, I'd love for you to share your feedback on our public discussion here:

https://github.com/418sec/huntr/discussions/2214

It helps us centralise your thoughts and feedback, and address them ASAP.

I will address the severity for you now 👍

Minh 7 months ago Researcher

@maintainer, @admin, could you please tell me why this bug is rated low Severity? seem not fair. other report on your project has the same attack vector, same impact and they have been rated high? for example: https://huntr.dev/bounties/16b0547b-1bb3-493c-8a00-5b6a11fca1c5/

Minh 7 months ago Researcher

here is my another report which has been rated low? https://huntr.dev/bounties/730eddfc-fe19-471d-acbb-c6ef8f079950/

Peter Ivanov 7 months ago

hi @admin can you change the severity to "low" as it requires admin access

Minh 7 months ago Researcher

hi @maintainer, could you please answer my question???

Peter Ivanov 7 months ago

hi, the bug is low severity as you need to be logged in as admin in order to reproduce it

Minh 7 months ago Researcher

the impact of this bug is steal admin cookie. when admin login and attacker
click this link, the admin cookie will be leak to the hacker, and the severity is
and in this report https://huntr.dev/bounties/16b0547b-1bb3-493c-8a00-5b6a11fca1c5/ have
exactly the same attack vector, you rated is high?

exactly the same attack vector, you rated is high?

Peter Ivanov 7 months ago

Hi, seems @bobimicroweber has tagged it as high severity by mistake

All bugs that require admin access should not be high severity

Minh 7 months ago Researcher

Seem not fair when you rated other report with same attack vector, same impact with high severity, and my report is low?

https://huntr.dev/bounties/16b0547b-1bb3-493c-8a00-5b6a11fca1c5/
https://huntr.dev/bounties/4999a0f4-6efb-4681-b4ba-b36babc366f9/
https://huntr.dev/bounties/d184ce19-9608-42f1-bc3d-06ece2d9a993/
https://huntr.dev/bounties/16b0547b-1bb3-493c-8a00-5b6a11fca1c5/
https://huntr.dev/bounties/085aafdd-ba50-44c7-9650-fa573da29bcd/
...

Peter Ivanov 7 months ago

hi, all those bugs are tagged as high by mistake, anyway keep this as high if you wish, just in the future admin bugs will be tagged as meduim/low

Minh 7 months ago Researcher

i don't need the bounty, but your explaination when you mark my report as low severity is not fair. here is the CVSS i caculate for you: AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:L at least it have the medium severity

Jamie Slome 7 months ago Admin

@peter-mw - can you let me know the CVSS vector for the low severity that you would like to set to this report?

@minhnb11 - please respect the maintainer's decision for this report (ultimately it is final). Any spam or harassment will not be accepted - if you do have any issues, please address them respectfully. If you believe there is something we can do better from a platform [illegible] free to create an issue on our public roadmap here.

Minh 7 months ago Researcher

@admin @maintainer, i'm fully respect the maintainer, just not agree if this report mark severity as low without explaination.

Sign in to join this conversation