[<prev] [next>] [day] [month] [year] [list]

```
Date: Tue, 14 Dec 2021 12:29:20 -0800
From: Aaron Patterson <aaron.patterson@...il.com>
To: oss-security@...ts.openwall.com, rubyonrails-security@...glegroups.com,
        ruby-security-ann@...glegroups.com
Subject: [CVE-2021-44528] Possible Open Redirect in Host Authorization Middleware

There is a possible open redirect vulnerability in the Host Authorization
middleware in Action Pack. This vulnerability has been assigned the CVE
identifier CVE-2021-44528.

Versions Affected:  >= 6.0.0.
Not affected:       < 6.0.0
Fixed Versions:     6.1.4.2, 6.0.4.2, 7.0.0.rc2

Impact
------
Specially crafted "X-Forwarded-Host" headers in combination with certain
"allowed host" formats can cause the Host Authorization middleware in Action
Pack to redirect users to a malicious website.

Impacted applications will have allowed hosts with a leading dot. For
example,
configuration files that look like this:

```
config.hosts <<  '.EXAMPLE.com'
```

When an allowed host contains a leading dot, a specially crafted Host header
can be used to redirect to a malicious website.

This vulnerability is similar to CVE-2021-22881 and CVE-2021-22942.

Releases

The fixed releases are available at the normal locations.

Patches

To aid users who aren't able to upgrade immediately we have provided
patches for
the two supported release series. They are in git-am format and consist of a
single changeset.

* 6-0-host-authorzation-open-redirect.patch - Patch for 6.0 series
* 6-1-host-authorzation-open-redirect.patch - Patch for 6.1 series
* 7-0-host-authorzation-open-redirect.patch - Patch for 7.0 series

Please note that only the 6.1.Z, 6.0.Z, and 5.2.Z series are supported at
present. Users of earlier unsupported releases are advised to upgrade as
soon
as possible as we cannot guarantee the continued availability of security
fixes for unsupported releases.

Credits

Thanks to [@krynos](https://hackerone.com/krynos?type=user) for originally
reporting this!

Huge thanks to
[@stefschenkelaars](https://hackerone.com/stefschenkelaars?type=user) for
writing a patch along with tests to fix this issue!

--
Aaron Patterson
http://tenderlovemaking.com/
```

Content of type "text/html**" skipped**

Download attachment "6-0-host-authorzation-open-redirect.patch**" of type "**application/octet-stream**" (6033 bytes)**

Download attachment "6-1-host-authorzation-open-redirect.patch**" of type "**application/octet-stream**" (6123 bytes)**

Download attachment "7-0-host-authorzation-open-redirect.patch**" of type "**application/octet-stream**" (6123 bytes)**