[CVE-2021-22904] Possible DoS Vulnerability in Action Controller Token Authentication

Aaron Patterson tenderlove core team **May '21**

There is a possible DoS vulnerability in the Token Authentication logic in Action Controller. This vulnerability has been assigned the CVE identifier CVE-2021-22904.

Versions Affected: >= 4.0.0 Not affected: < 4.0.0 Fixed Versions: 6.1.3.2, 6.0.3.7, 5.2.4.6, 5.2.6

Impact

Impacted code uses `authenticate_or_request_with_http_token` or `authenticate_with_http_token` for request authentication. Impacted code will look something like this:

```
class PostsController < ApplicationController
  before_action :authenticate

  private

  def authenticate
    authenticate_or_request_with_http_token do |token, options|
      # ...
    end
  end
end
```

All users running an affected release should either upgrade or use one of the workarounds immediately.

Releases

The fixed releases are available at the normal locations.

Workarounds

The following monkey patch placed in an initializer can be used to work around the issue:

```
module ActionController::HttpAuthentication::Token
  AUTHN_PAIR_DELIMITERS = /(?:,|;|\t)/
end
```

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.

- 5-2-http-authentication-dos.patch - Patch for 5.2 series
- 6-0-http-authentication-dos.patch - Patch for 6.0 series
- 6-1-http-authentication-dos.patch - Patch for 6.1 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

Thank you to HackerOne for reporting this issue!

6-1-http-authentication-dos.patch (2.1 KB) **6-0-http-authentication-dos.patch** (2.1 KB)
5-2-http-authentication-dos.patch (2.1 KB)