WWBN / AVideo Public

Code Issues 13 Pull requests Actions Projects Wiki Security a

Commit a0156a6

Daniel Neto committed last week · 11 / 11

```
fix: Improve SSRF protection by enforcing same-origin requests with matching hostname and port

GHSA-j432-4w3j-3w8j
```

master

1 parent 80f38a5 commit a0156a6

1 file changed +12 -4 lines changed

Top

Filter files…

objects

functions.php

1 file changed +12 -4 lines changed

Search within code

objects/functions.php

```
@@ -4304,11 +4304,19 @@ function isSSRFSafeURL($url, &$resolvedIP = null)
4304 4304
4305 4305         $host = strtolower($host);
4306 4306
4307      -     // Allow loopback/private IPs if the URL points to the same domain as webSiteRootURL
     4307 +     // Allow requests to the same origin as webSiteRootURL (hostname + port must both match).
     4308 +     // Checking hostname only is insufficient: an attacker can reach arbitrary internal ports
     4309 +     // on the same host by using the site's public hostname with a non-standard port.
```

```
4308  4310          if (!empty($global['webSiteRootURL'])) {
4309        -         $siteHost = strtolower(parse_url($global['webSiteRootURL'],
                    PHP_URL_HOST));
4310        -         if ($host === $siteHost) {
4311        -             _error_log("isSSRFSafeURL: allowing same-domain request to
                    {$host} (matches webSiteRootURL)");
            4311  +   $siteHost   = strtolower(parse_url($global['webSiteRootURL'],
                    PHP_URL_HOST));
            4312  +   $siteScheme = strtolower(parse_url($global['webSiteRootURL'],
                    PHP_URL_SCHEME) ?: 'http');
            4313  +   $sitePort   = (int)(parse_url($global['webSiteRootURL'],
                    PHP_URL_PORT) ?: ($siteScheme === 'https' ? 443 : 80));
            4314  +
            4315  +   $urlScheme = strtolower(parse_url($url, PHP_URL_SCHEME) ?: 'http');
            4316  +   $urlPort   = (int)(parse_url($url, PHP_URL_PORT) ?: ($urlScheme ===
                    'https' ? 443 : 80));
            4317  +
            4318  +   if ($host === $siteHost && $urlPort === $sitePort) {
            4319  +       _error_log("isSSRFSafeURL: allowing same-origin request to
                    {$host}:{$urlPort} (matches webSiteRootURL)");
4312  4320              return true;
4313  4321          }
4314  4322      }
```

Comments 0

Please sign in to comment.