



# CVE-2023-27592

Published on: Not Yet Published

Last Modified on: 03/24/2023 04:28:00 PM UTC

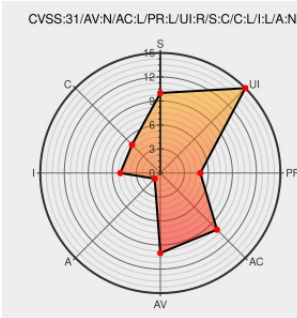
## CVE-2023-27592 - advisory for GHSA-mqqg-xjhj-wfgw

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Miniflux](#) from [Miniflux Project](#) contain the following vulnerability:

Miniflux is a feed reader. Since v2.0.25, Miniflux will automatically proxy images served over HTTP to prevent mixed content errors. When an outbound request made by the Go HTTP client fails, the `html.ServerError` is returned unescaped without the expected Content Security Policy header added to valid responses. By creating an RSS

feed item with the inline description containing an `<img>` tag with a `srcset` attribute pointing to an invalid URL like `http:a<script>alert(1)</script>`, we can coerce the proxy handler into an error condition where the invalid URL is returned unescaped and in full. This results in JavaScript execution on the Miniflux instance as soon as the user is convinced (e.g. by a message in the alt text) to open the broken image. An attacker can execute arbitrary JavaScript in the context of a victim Miniflux user when they open a broken image in a crafted RSS feed. This can be used to perform actions on the Miniflux instance as that user and gain administrative access to the Miniflux instance if it is reachable and the victim is an administrator. A patch is available in version 2.0.43. As a workaround disable image proxy; default value is `http-only`.

CVE-2023-27592 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **miniflux** - v2 version = `>= 2.0.25, < 2.0.43`

CVSS3 Score: **5.4 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
<b>NETWORK</b>	<b>LOW</b>	<b>LOW</b>	<b>REQUIRED</b>
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
<b>CHANGED</b>	<b>LOW</b>	<b>LOW</b>	<b>NONE</b>

## CVE References

Description	Tags	Link
Configuration Parameters	<a href="#">miniflux.app</a> <a href="#">text/html</a>	 MISC <a href="https://miniflux.app/docs/configuration.html#proxy-images">miniflux.app/docs/configuration.html#proxy-images</a>
Stored XSS in Miniflux when opening a broken image due to unescaped ServerError in proxy handler · Advisory · miniflux/v2 · GitHub	<a href="#">github.com</a> <a href="#">text/html</a>	 MISC <a href="https://github.com/miniflux/v2/security/advisories/GHSA-mqqg-xjhj-wfgw">github.com/miniflux/v2/security/advisories/GHSA-mqqg-xjhj-wfgw</a>
Release Miniflux 2.0.43 · miniflux/v2 · GitHub	<a href="#">github.com</a> <a href="#">text/html</a>	 MISC <a href="https://github.com/miniflux/v2/releases/tag/2.0.43">github.com/miniflux/v2/releases/tag/2.0.43</a>
v2/proxy.go at b2fd84e0d376a3af6329b9bb2e772ce38a25c31c · miniflux/v2 · GitHub	<a href="#">github.com</a> <a href="#">text/html</a>	 MISC <a href="https://github.com/miniflux/v2/blob/b2fd84e0d376a3af6329b9bb2e772ce38a25c31c">github.com/miniflux/v2/blob/b2fd84e0d376a3af6329b9bb2e772ce38a25c31c</a>
v2/proxy.go at b2fd84e0d376a3af6329b9bb2e772ce38a25c31c · miniflux/v2 · GitHub	<a href="#">github.com</a> <a href="#">text/html</a>	 MISC <a href="https://github.com/miniflux/v2/blob/b2fd84e0d376a3af6329b9bb2e772ce38a25c31c">github.com/miniflux/v2/blob/b2fd84e0d376a3af6329b9bb2e772ce38a25c31c</a>
Avoid XSS when opening a broken image due to unescaped ServerError in proxy handler by fguiilot · Pull Request #1746 · miniflux/v2 · GitHub	<a href="#">github.com</a> <a href="#">text/html</a>	 MISC <a href="https://github.com/miniflux/v2/pull/1746">github.com/miniflux/v2/pull/1746</a>
Release Miniflux 2.0.25 · miniflux/v2 · GitHub	<a href="#">github.com</a> <a href="#">text/html</a>	 MISC <a href="https://github.com/miniflux/v2/releases/tag/2.0.25">github.com/miniflux/v2/releases/tag/2.0.25</a>

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).



There are currently no QIDs associated with this CVE

## Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Miniflux Project</a>	Miniflux	All	All	All	All
<code>cpe:2.3:a:miniflux_project:miniflux:*:*:*:*:go:*:*:</code>						

No vendor comments have been submitted for this CVE

## Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2023-27592 : Miniflux is a feed reader. Since v2.0.25, Miniflux will automatically proxy images served over HTT... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a>	2023-03-17 20:04:49
 /r/netcve	<a href="#">CVE-2023-27592</a>	2023-03-17 20:38:47

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)**