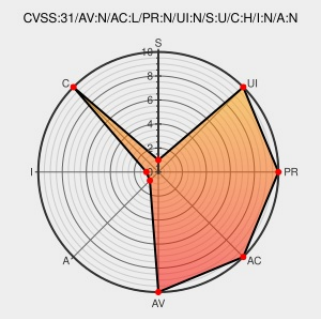
CVE-2023-27591

Published on: Not Yet Published

Last Modified on: 03/24/2023 02:50:00 PM UTC

CVE-2023-27591 - advisory for GHSA-3qjf-qh38-x73v

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Miniflux from Miniflux Project contain the following vulnerability:

Miniflux is a feed reader. Prior to version 2.0.43, an unauthenticated user can retrieve Prometheus metrics from a publicly reachable Miniflux instance where the `METRICS_COLLECTOR` configuration option is enabled and `METRICS_ALLOWED_NETWORKS` is set to `127.0.0.1/8` (the default). A patch is available in Miniflux 2.0.43. As a workaround, set `METRICS_COLLECTOR` to `false` (default) or run Miniflux behind a trusted reverse-proxy.

CVE-2023-27591 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **miniflux** - **v2** version **= < 2.0.43**

CVSS3 Score: 7.5 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	NONE	NONE

CVE References

Description	Tags	Link
Release Miniflux 2.0.43 · miniflux/v2 · GitHub	github.com text/html	MISC github.com/miniflux/v2/releases/tag/2.0.43
Configuration Parameters	miniflux.app text/html	MISC miniflux.app/docs/configuration.html#metrics-collector
Unauthenticated user can bypass allowed networks check to obtain Prometheus metrics · Advisory · miniflux/v2 · GitHub	github.com text/html	MISC github.com/miniflux/v2/security/advisories/GHSA-3qjf-qh38-x73v

Use `r.RemoteAddr` to check `/metrics` endpoint network access by fguillot · Pull Request #1745 · miniflux/v2 · GitHub	github.com text/html	MISC github.com/miniflux/v2/pull/1745

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Miniflux Project	Miniflux	All	All	All	All

cpe:2.3:a:miniflux_project:miniflux:*:*:*:*:*:go:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2023-27591 : Miniflux is a feed reader. Prior to version 2.0.43, an unauthenticated user can retrieve Prometheu… twitter.com/i/web/status/1…	2023-03-17 20:04:27
/r/netcve	CVE-2023-27591	2023-03-17 20:38:46

← Previous ID

Next ID→