

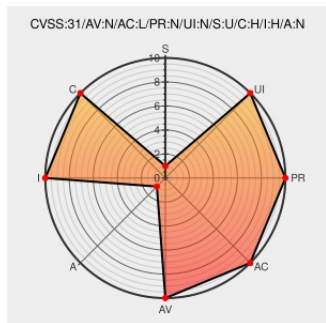


CVE-2020-15097

Published on: 02/02/2021 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:42 PM UTC

CVE-2020-15097 - advisory for GHSA-7557-4v29-rqw6

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

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

loklak is an open-source server application which is able to collect messages from various sources, including twitter. The server contains a search index and a peer-to-peer index sharing interface. All messages are stored in an elasticsearch index. In loklak less than or equal to commit 5f48476, a path traversal vulnerability exists.

Insufficient input validation in the APIs exposed by the loklak server allowed a directory traversal vulnerability. Any admin configuration and files readable by the app available on the hosted file system can be retrieved by the attacker. Furthermore, user-controlled content could be written to any admin config and files readable by the application. This has been patched in commit 50dd692. Users will need to upgrade their hosted instances of loklak to not be vulnerable to this exploit.

CVE-2020-15097 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: [Loklak](#) - loklak version <= 5f48476d6f06dc00d87d25def5f789db703dfe3e

CVSS3 Score: **9.1 - CRITICAL**

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

CVSS2 Score: **6.4 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality	Integrity	Availability

Confidentiality Impact

PARTIAL

Integrity Impact

PARTIAL

Availability Impact

NONE

CVE References

Description	Tags	Link
Vulnerability - Directory Traversal Attacks in Loklak Instances · Advisory · loklak/loklak_server · GitHub	Third Party Advisory github.com text/html	CONFIRM github.com/loklak/loklak_server/security/advisories/GHSA-7557-4v29-rqw6
Merge pull request from GHSA-7557-4v29-rqw6 · loklak/loklak_server@50dd692 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/loklak/loklak_server/commit/50dd69230d3cd71dab0bfa7156682ffeca8ed8t

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:loklak_project:loklak:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →