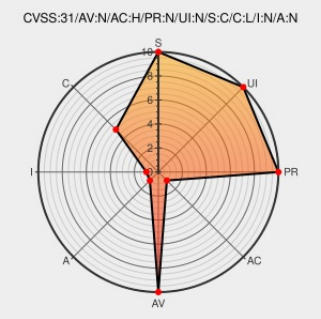
CVE-2022-1561

Published on: Not Yet Published

Last Modified on: 08/08/2022 01:24:00 PM UTC

CVE-2022-1561

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



Certain versions of Krakend from Krakend contain the following vulnerability:

Lura and KrakenD-CE versions older than v2.0.2 and KrakenD-EE versions older than v2.0.0 do not sanitize URL parameters correctly, allowing a malicious user to alter the backend URL defined for a pipe when remote users send crafty URL requests. The vulnerability does not affect KrakenD itself, but the consumed backend might be vulnerable.

CVE-2022-1561 has been assigned by cve-coordination@incibe.es to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **KrakenD** - **Lura Project** version **< v2.0.2**

Affected Vendor/Software: **KrakenD** - **KrakenD-CE** version **< v2.0.2**

Affected Vendor/Software: **KrakenD** - **KrakenD-EE** version **< v2.0.0**

CVSS3 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
Crafted backend URLs in Lura Project | INCIBE-CERT	www.incibe-cert.es text/html	CONFIRM www.incibe-cert.es/en/early-warning/security-advisories/crafted-backend-urls-lura-project
CVE-2022-1561: Crafted backend urls - KrakenD API Gateway	www.krakend.io text/html	CONFIRM www.krakend.io/blog/cve-2022-1561-crafted-backend-urls/

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	Krakend	Krakend	All	All	All	All
Application	Krakend	Krakend	All	All	All	All
Application	Luraproject	Lura	All	All	All	All

cpe:2.3:a:krakend:krakend:*:*:*:*:enterprise:*:*:*:

cpe:2.3:a:krakend:krakend:*:*:*:*:community:*:*:*:

cpe:2.3:a:luraproject:lura:*:*:*:*:*:*:*:*:

Discovery Credit

Discovered by Github user Fepame

Social Mentions

Source	Title	Posted (UTC)
@incibe_cert	⚠ Alteración de URL del backend en #LuraProject #CNA #0day #CVE CVE-2022-1561 incibe-cert.es/alerta-tempran…	2022-07-29 06:28:54
@CVEreport	CVE-2022-1561 : Lura and KrakenD-CE versions older than v2.0.2 and KrakenD-EE versions older than v2.0.0 do not san… twitter.com/i/web/status/1…	2022-08-01 13:08:15
/r/netcve	CVE-2022-1561	2022-08-01 14:38:23

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report