Home / Advisories / PartKeepr v1.4.0 url attachment 'add parts' SSRF

PartKeepr v1.4.0 url attachment 'add parts' - SSRF

Summary

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you’ve provided to them or that they’ve collected from your use of their services. You consent to our cookies if you continue to use our website.

Allow all cookies

Show details

Versions	v1.4.0
State	Public
Release date	2022-01-09

Vulnerability

Kind	Server Side Request Forgery
Rule	100. Server-side request forgery (SSRF)
Remote	Yes
CVSSv3 Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N
CVSSv3 Base Score	4.3
Exploit available	No
CVE ID(s)	CVE-2022-22702

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

Allow all cookies

Show details

Proof of Concept

- Go to 'Add Part'.
- Click on 'Attachments'.
- Click on 'Add'.
- Fill the 'URL' field with an url using a local port "http://127.0.0.1:3306".
- Click on 'Upload'.
- Click on the uploaded file in order to download the file and see the content.

Exploit

There is no exploit for the vulnerability but can be manually exploited.

Mitigation

By 2022-01-04 there is not a patch resolving the issue.

Credits

The vulnerability was discovered by Oscar Uribe from the Offensive Team of `Fluid Attacks`.

References

Vendor page https://partkeepr.org/

Issue https://github.com/partkeepr/PartKeepr/issues/1230/

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

Allow all cookies

Show details

✓ Vendor contacted.

✓ 2022-01-09
Public Disclosure.

Services

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

Allow all cookies

Show details

DevSecOps

Secure Code Review

Red Teaming

Breach and Attack Simulation

Security Testing

Penetration Testing

Ethical Hacking

Vulnerability Management

Blog

Certifications

Partners

Careers

Advisories

FAQ

Documentation

Contact

Copyright © 2022 Fluid Attacks. We hack your software. All rights reserved.

Service Status - Terms of Use - Privacy Policy - Cookie Policy

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

Allow all cookies

Show details