Browsershot 3.57.2 - Server Side XSS to LFR via HTML

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

Affected versions	Version 3.57.2
State	Public
Release date	2022-10-28

Vulnerability

Kind	Server Side XSS
Rule	425. Server Side XSS
Remote	Yes
CVSSv3 Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
CVSSv3 Base Score	7.5
Exploit available	Yes
CVE ID(s)	CVE-2022-43983

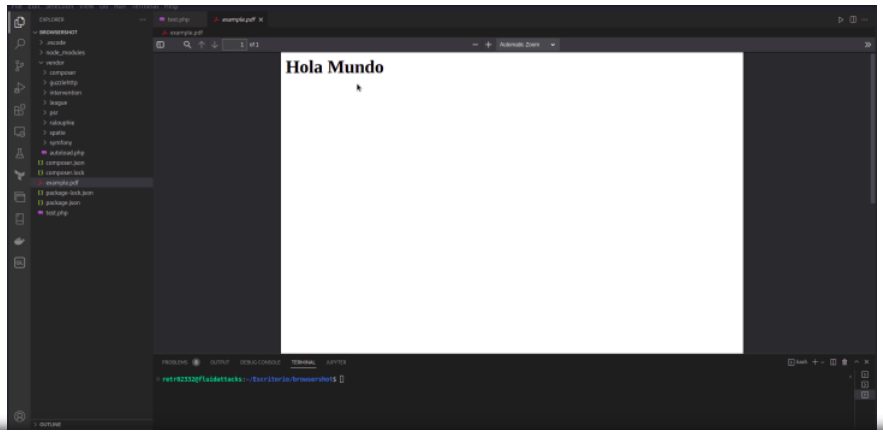
Description

Browsershot version 3.57.2 allows an external attacker to remotely obtain arbitrary local files. This is possible because the application does not validate that the HTML content passed to the `Browsershot::html` method does not contain URL's that use the `file://` protocol.

Vulnerability

This vulnerability occurs because the application does not validate that the HTML content passed to the `Browsershot::html` method does not contain URL's that use the `file://` protocol.

Exploitation

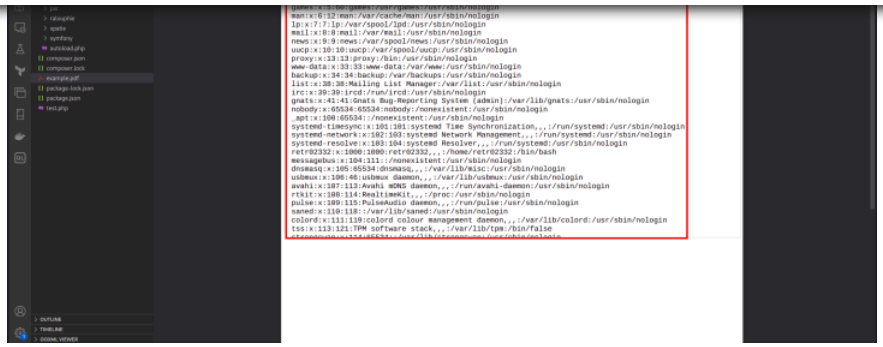


This website uses cookies

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



Our security policy

We have reserved the CVE-2022-43983 to refer to these issues from now on.

- https://fluidattacks.com/advisories/policy/

System Information

- Version: Browsershot 3.57.2
- Operating System: GNU/Linux

Mitigation

An updated version of Browsershot is available at the vendor page.

Credits

The vulnerability was discovered by Carlos Bello from Fluid Attacks' Offensive Team.

References

Vendor page https://github.com/spatie/browsershot

Release https://github.com/spatie/browsershot/releases/tag/3.57.3

Timeline

2022-10-25
Vulnerability discovered.

2022-10-25
Vendor contacted.

2022-10-25
Vendor replied acknowledging the report.

2022-10-25

Vendor Confirmed the vulnerability.

2022-10-25
Vulnerability patched.

2022-10-28
Public Disclosure.

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

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