Browsershot 3.57.3 - Server Side XSS to LFR via HTML

Summary

Affected versions	Version 3.57.3
State	Public
Release date	2022-11-21

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-2022-43984

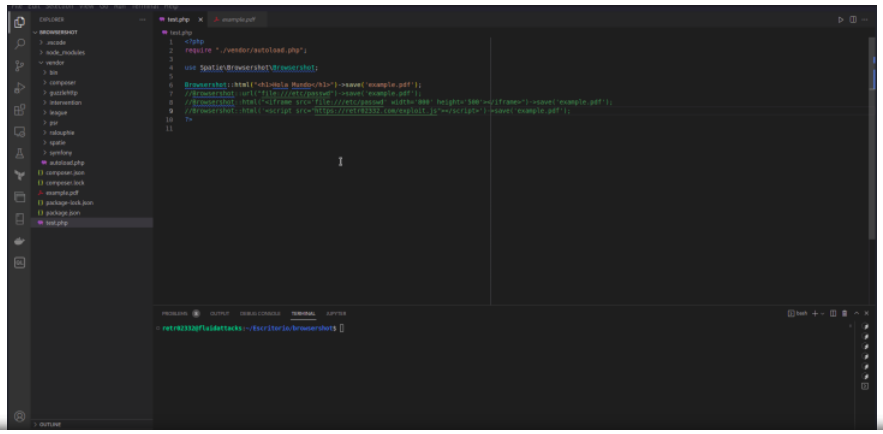
Description

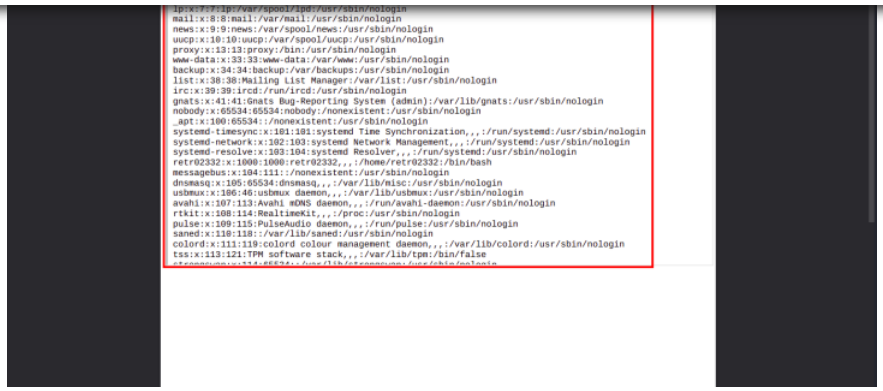
Browsershot version 3.57.3 allows an external attacker to remotely obtain arbitrary local files. This is possible because the application does not validate that the JS content imported from an external source passed to the `Browsershot::html` method does not contain URLs that use the `file://` protocol.

Vulnerability

This vulnerability occurs because the application does not validate that the JS content imported from an external source passed to the `Browsershot::html` method does not contain URLs that use the `file://` protocol.

Evidence of exploitation





Our security policy

We have reserved the CVE-2022-43984 to refer to these issues from now on.

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

System Information

- Version: Browsershot 3.57.3
- 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

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.

2022-11-21
Public Disclosure.