



Browsershot 3.57.3 – 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 3.57.3

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

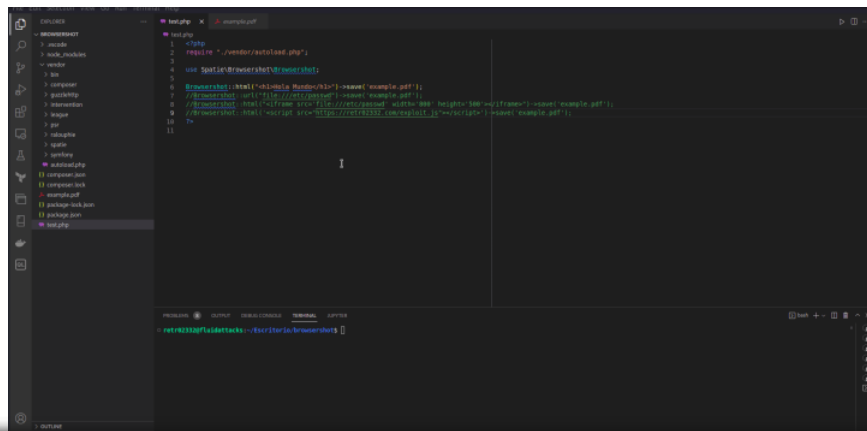
Description

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



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

```
ip:x:7:7:ip:/var/spool/ipp:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mail list Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:101:systemd Time Synchronization,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,:/run/systemd:/usr/sbin/nologin
retro232:x:1000:1000:retro232,,:/home/retro232:/bin/bash
messagebus:x:104:111::/nonexistent:/usr/sbin/nologin
dnsmasq:x:105:65534:dnsmasq,,:/var/lib/misc:/usr/sbin/nologin
usbmux:x:106:46:usbmux daemon,,:/var/lib/usbmux:/usr/sbin/nologin
avahi:x:107:113:Avahi mDNS daemon,,:/run/avahi-daemon:/usr/sbin/nologin
rtkit:x:108:114:RealtimeKit,,:/proc:/usr/sbin/nologin
pulse:x:109:115:PulseAudio daemon,,:/run/pulse:/usr/sbin/nologin
saned:x:110:118:/var/lib/saned:/usr/sbin/nologin
colord:x:111:119:colord colour management daemon,,:/var/lib/colord:/usr/sbin/nologin
tss:x:113:121:TPM software stack,,:/var/lib/tpm:/bin/false
systemd-user:x:114:114:systemd user:/etc/passwd:/usr/sbin/nologin
```

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.



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](#)

Services

[Continuous Hacking](#)

[One-shot Hacking](#)

[Comparative](#)

Solutions

[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