	Authorisation. Jason Edelstein
	Release date. 23 February 2009.

Sense of Security – Security Advisory – SOS-09-001.

Libero Cross-Site Scripting Vulnerability.

23 February 2009.

Libero Cross-Site Scripting Vulnerability - Security Advisory – SOS-09-001

Release Date.	23-Feb-2009
Last Update.	-
Vendor Notification Date.	20-Oct-2008
Product.	Libero
Platform.	Windows (verified), possibly others
Affected versions.	Libero v5.3 SP5 (verified), possibly others
Severity Rating.	Medium
Impact.	Cookie/credential theft, impersonation, loss of confidentiality
Attack Vector.	Remote
Solution Status.	Vendor patch not yet available
CVE reference.	CVE-2009-0540

Details.

Libero is a library management system. During an application penetration test Sense of Security identified a cross-site scripting vulnerability in the search feature of the Libero web application. This occurred as a result of the application not properly filtering HTML tags which allowed malicious Javascript to be embedded. When input is incorrectly validated and not properly sanitised and then displayed in a web page, attackers can trick users into viewing the web page and causing malicious code to be executed.

Proof of Concept.

You can test the susceptibility of your system to this issue by entering the following string into the search term form field and clicking ‘search’.

```
<script>alert(document.cookie)</script>
```

A vulnerable site will return the users’ session ID.

Solution.

The vendor has advised that the fix will be made available in Libero v5.5 SP1.

A fix will not be made available for previous versions.

Discovered by.

Oliver Greiter from SOS Labs.

About us.

Sense of Security is a leading provider of IT security and risk management solutions. Our team has expert skills in assessment and assurance, strategy and architecture, and deployment through to ongoing management. We are Australia’s premier application security consultancy and trusted IT security advisor to many of the countries largest organisations.

Sense of Security Pty Ltd

Level 3, 66 King St
Sydney NSW 2000
AUSTRALIA

T: +61 (0)2 9290 4444
F: +61 (0)2 9290 4455
W: http://www.senseofsecurity.com.au
E: info@senseofsecurity.com.au