



Authorisation.

Jason Edelstein

Release date.
12 March 2012.

Sense of Security – Security Advisory – SOS-12-004.
Aurora WebOPAC SQL Injection Vulnerability.
12 March 2012.

© Sense of Security 2012.	Editor Jason Edelstein.	Page No 1.
www.senseofsecurity.com.au	All rights reserved.	Version 1.0.



Authorisation.

Jason Edelstein

Release date.

12 March 2012.

Aurora WebOPAC SQL Injection - Security Advisory - SOS-12-004

Release Date.	12-Mar-2012
Last Update.	-
Vendor Notification Date.	24-Nov-2011
Product.	Aurora WebOPAC
Platform.	Independent
Affected versions.	3.5.0e, 3.4.6a, 3.5.3, 3.5.0i, 3.4.7b, 3.5.2.2, 3.4.7b, possibly others
Severity Rating.	High
Impact.	Exposure of sensitive information
Attack Vector.	From remote without authentication
Solution Status.	Vendor patch
CVE reference.	CVE- not yet assigned

Details.

Aurora WebOPAC is an online library system which allows users to perform tasks, such as reservations, renewal of books, search the catalogue, etc.

During an application penetration test Sense of Security identified that Aurora WebOPAC suffers from SQL injection vulnerabilities in MemberDetailsRecovery.aspx, as it fails to validate data supplied in the 'txtEmailAliasBarcode' variable before being used in a SQL query.

Solution.

The vendor has advised that Patch R.3.5.3 is available, and should be applied to fix the issue.

© Sense of Security 2012.	Editor Jason Edelstein.	Page No 2.
www.senseofsecurity.com.au	All rights reserved.	Version 1.0.



Authorisation.

Jason Edelstein

Release date.

12 March 2012.

Discovered by.

Niket Khosla from Sense of Security Labs.

About us.

Sense of Security is a leading provider of information 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 penetration testing firm and trusted IT security advisor to many of the country's largest organisations.

Sense of Security Pty Ltd

Level 8, 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

Twitter: @ITsecurityAU

The latest version of this advisory can be found at:

<http://www.senseofsecurity.com.au/advisories/SOS-12-004.pdf>

Other Sense of Security advisories can be found at:

<http://www.senseofsecurity.com.au/research/it-security-advisories.php>

© Sense of Security 2012.	Editor Jason Edelstein.	Page No 3.
www.senseofsecurity.com.au	All rights reserved.	Version 1.0.