Sense of Security	Authorisation. Jason Edelstein
	Release date. 17 August 2009.

Sense of Security – Security Advisory – SOS-09-007.

Piwigo SQL Injection Vulnerability.

17 August 2009.

Piwigo SQL Injection Vulnerability - Security Advisory - SOS-09-007

Release Date.	17-Aug-2009
Last Update.	-
Vendor Notification Date.	15-Jun-2009
Product.	Piwigo
Platform.	Independent
Affected versions.	2.0.0 (verified), possibly others
Severity Rating.	Medium
Impact.	Manipulation of data
Attack Vector.	Remote without authentication
Solution Status.	Upgrade to 2.0.3
CVE reference.	Not yet assigned

Details.

Piwigo is a photo gallery application written in PHP. The application suffers from a SQL injection vulnerability in comments.php, as it fails to validate data supplied in the “items_number” variable before being used in an SQL query.

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.

/piwigo-2.0.0/comments.php?items_number=1’”

Solution.

Upgrade to version 2.0.3.

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 firm 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-09-007.pdf

Other Sense of Security advisories can be found at:

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