SINTELLI
INTELLIGENT SECURITY

SQL Injection Vulnerability in FuzzyMonkey MyClassifieds SQL Version

18 October 2003

Background

My Classifieds SQL is a Perl/CGI/MySQL script which will quickly and easily allow the hosting of a classifieds forum on a website.

.

More information about the product is available here:
http://fuzzymonkey.org/newfuzzy/software/perl/classifieds/readme.html

Description

MyClassifieds SQL Version is vulnerable to a SQL injection attack. The problem is due to improper sanitization of user input for the $email variable. A remote attacker could insert arbitrary SQL code in the $email variable. The passwords of the users can be written into a file and made world readable.

Example:
If the value of $email is aaa@aaa.com' OR 1=1 INTO OUTFILE '/<directory-path>/pass.txt, the SQL request becomes:

select passmd5 from people where email=' aaa@aaa.com' OR 1=1 INTO OUTFILE '/<directory-path>/pass.txt'

and the passwords of the users can be written into the file pass.txt.

Impact

It is possible for an attacker to obtain passwords of users.

Versions affected

Version 2.11

Solution

Upgrade to version 2.13
http://www.fuzzymonkey.org/files/myclassifiedssql-2.13.tar.gz

Vulnerability History

15 Oct 2003	Identified by Ezhilan of Sintelli
15 Oct 2003	Issue disclosed to FuzzyMonkey (Erin)
16 Oct 2003	Vulnerability confirmed by Erin
18 Oct 2003	Fix available
18 Oct 2003	Sintelli confirms vulnerability has been addressed
18 Oct 2003	Sintelli Public Disclosure

Credit

Ezhilan of Sintelli discovered this vulnerability.

About Sintelli:

Sintelli is the world's largest provider of security intelligence solutions. Sintelli is the definitive source for IT Security intelligence and is a provider of third generation intelligence security solutions.

Request a free trial of our alerting solution by clicking here http://www.sintelli.com/free-trial.htm