

[VulnWatch] [AppSecInc Advisory MYSQL05-V0003] Multiple Issues with MySQL User Defined Functions

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2005-08/0005.html>

From: Team SHATTER (*shatter_at_appsecinc.com*)

Date: 08/09/05

Date: Mon, 08 Aug 2005 18:41:59 -0400

To: bugtraq@securityfocus.com

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Multiple Issues with MySQL User Defined Functions

AppSecInc Team SHATTER Security Advisory MYSQL05-V0003

<http://www.appsecinc.com/resources/alerts/mysql/2005-003.html>

August 08, 2005

Risk level: LOW

Credits: This vulnerability was discovered and researched by Reid Borsuk of Application Security Inc.

Affected Versions:

ALL

Background:

User-defined functions in MySQL allow a user in the database to call binary libraries on the operating system. Creating a user-defined function requires insert privileges on the mysql.func table.

Details:

By using specially crafted CREATE FUNCTION requests it may be possible for attackers to halt the system or execute remote code on some systems. Two specific issues are detailed below.

1) If an attacker asks a Windows based MySQL server to load an invalid library file the application will hang until a dialog box is acknowledged on the server. By requesting one of the many non-library files included in the PATH by default on Windows installations a server will be effectively halted. This is due to the fact that the Windows function LoadLibraryEx() will block when loading an invalid

library file with the following message:

"The application or DLL XXXX is not a valid Windows image. Please check this against your installation diskette."

It should be noted that this is a Windows specific issue; other operating systems are not likely to be affected.

An attacker attempting to exploit this issue must have insert privileges on the mysql.func table. This is a high level of privilege that is not normally given to untrusted users.

2) MySQL attempts to filter execution of arbitrary libraries by requiring any UDF libraries to have either XXX_deinit() or XXX_init() functions defined. This is intended to prevent an attacker from including any libraries that were not specifically programmed to work with MySQL. Unfortunately this function naming convention is relatively common and default libraries may have these functions defined.

For instance, the "jpeg1x32.dll" and "jpeg2x32.dll" libraries, included by default with Windows 2000 have these functions defined. This allows an attacker to load the jpeg_cmp() function from "jpeg1x32.dll" and the jpeg_decmp() function from "jpeg2x32.dll". When either of these functions is called, the MySQL daemon will crash due to improper argument passing.

Both the jpeg_cmp_init() and jpeg_decmp_init() functions assumes there are 6 arguments waiting for it on the stack. One of these, Arg 6 (EBP+0x1C) is assumed to be a pointer to a memory location. Areas of the memory past this pointer are later overwritten by other arguments passed to this function. Due to the fact that Arg 4 (EBP+0x14) through Arg 6 (EBP+0x1C) are not used prior to this call, it may be possible to pollute the stack and overwrite arbitrary memory locations with attacker supplied values.

Although this is a Windows specific example, it is possible that other operating systems are affected.

Exploiting this vulnerability would require the ability to create user-defined functions. This is not typically granted to untrusted users, however given this vulnerability you should understand the ramifications of granting the ability to create user-defined functions.

Workaround:

Restrict access to create user-defined functions.

Vendor Status:

Vendor was contacted and declined to produce a patch.

Fix:

None is available.

Links:

Application Security, Inc advisory:

<http://www.appsecinc.com/resources/alerts/mysql/2005-003.html>

-- --

Application Security, Inc.

www.appsecinc.com

AppSecInc is the leading provider of database security solutions for the enterprise. AppSecInc products proactively secure enterprise applications at more than 300 organizations around the world by discovering, assessing, and protecting the database against rapidly changing security threats. By securing data at its source, we enable organizations to more confidently extend their business with customers, partners and suppliers. Our security experts, combined with our strong support team, deliver up-to-date application safeguards that minimize risk and eliminate its impact on business.

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.4.0 (MingW32)

iD8DBQFC99+2/0w1dSVRt4URAOjuAKCq878ITG4qdH7yy9BCLfvV7SUotACgxjUX
RG9CbBZAo3R3eOdkV73g7I=
=0sOE

-----END PGP SIGNATURE-----