

Brinkster Multiple Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2004-02/0235.html>

From: Ferruh Mavituna (ferruh_at_mavituna.com)

Date: 02/09/04

To: <bugtraq@securityfocus.com>

Date: Mon, 9 Feb 2004 22:44:34 +0200

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

Hash: SHA1

BRINKSTER MULTIPLE VULNERABILITIES

Online URL : <http://ferruh.mavituna.com/article/?435>

1. Retrieving other users ASP Source Codes

Severity: Highly Critical

2. Accessing Database Files

Severity: Medium Critical

3. Skipping Brinkster Code Controls

Severity: Low Critical

ABOUT BRINKSTER;

Brinkster is a popular free and paid Windows based web hosting company with many customers www.brinkster.com

VULNURABLE;

Currently (1/26/2004) Brinkster.com is vulnerable;

1.RETRIEVING OTHER USERS ASP SOURCE CODES

Any valid user can access other users source codes just by know file names. So an attacker can access ASP Source Codes, database passwords and other information in source codes.

2. ACCESSING DATABASE FILES

If you know the name of any Brinkster user database file you can download it. (You can find database name form source code –see: first vuln.–). Brinkster use a spesific and accesible folder to store user database files.

3. SKIPPING CODE CONTROLS

Brinkster does not allow some code snippets in ASP files for server performance. Like "Server.Scripttimeout = 8000". Brinkster File Manager automatically scanning your uploaded source code and if it finds any restricted keyword, it will delete your uploaded file.

You can skip this by using ASP built–in Execute() function. This function is not in Brinkster keyword blacklist. So write a simple decoder and encoder for your code and use it by Execute() function.

HISTORY;

01.01.2004 – Discovered
01.18.2004 – Vendor Informed (twice)
02.08.2004 – Published

Vendor Status;

No answer;

Ferruh Mavituna
Web Application Security Specialist
<http://ferruh.mavituna.com>

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

Version: PGP 8.0.3

iQA/AwUBQCfxKzL0QoVzo2STEQJvNACgsL12jR67QCZh0INWbx/jVOs3uPIAn1PJ
lAbSYDuN+8DZGvayj9HmTj/C
=ICL6

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