

[NT] BetaParticle Database Disclosure and Arbitrary File Inclusion

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-05/0138.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 05/26/05

To: list@securiteam.com

Date: 26 May 2005 18:10:10 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

BetaParticle Database Disclosure and Arbitrary File Inclusion

SUMMARY

<<http://www.betaparticle.com/blog/index.html>> BetaParticle is "a simple to use ASP CMS (Blog + Gallery)".

Two vulnerabilities discovered in BetaParticle CMS. Exploiting these two vulnerabilities allows an attacker to reveal administrator's login information and to access system's files with the possibility to delete or upload new files.

DETAILS

Vulnerable Systems:

- * BetaParticle versions 3.0 and prior

Immune Systems:

- * BetaParticle version 4.0

Database Disclosure:

There is free access to database files, making its possible to download it and disclose the administrator username and password.

Securiteam: [NT] BetaParticle Database Disclosure and Arbitrary File Inclusion

Database path for versions prior to 3.0:

<http://example.com/bp/database/dbBlogMX.mdb>

Database path for version 3.0 and up: <http://example.com/Blog.mdb>

Workaround:

Move your DB to outside the web root and correct DB physical path.

Upload/Delete Arbitrary Files:

By accessing the following user interface, a remote attacker can initiate a upload mechanism without having to be logged on as administrator:

<http://example.com/bp/upload.asp>

By accessing the following user interface, a remote attacker can initiate the deletion of files without having to be logged on as administrator:

<http://example.com/bp/myFiles.asp>

ADDITIONAL INFORMATION

The information has been provided by <mailto:farhadkey@yahoo.com> farhad koosha.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.