



Security At The Source

CodeScan
software is
available now



Click here
to buy online

**Strengthening web
applications,
reducing security
related risk**

CONTACT DETAILS

Tel.: + 64 9 309 7650

Fax.: + 64 9 309 7651

info@codescan.com

Home	About Us	Product Info	Support	News
Overview	Latest News	Releases	Advisories	Contact

Avatar MOD v1.3 for Snitz Forums v3.4 - Arbitrary File Upload

```
=====
= CodeScan Advisory, codescan.com <advisories@codescan.com>
=
= Avatar MOD v1.3 for Snitz Forums v3.4 - Arbitrary File Upload
=
= Vendor Website:
= http://www.snitzbitz.com/mods/details.asp?Version=All&mid=52
=
= Affected Version:
= Avatar MOD v1.3 for Snitz Forums v3.4
=
= Researched By
= Paul Craig <paul.craig@security-assessment.com>
=
= Public disclosure on May 18th, 2006
=====
== Overview ==
```

CodeScan Labs (www.codescan.com), has recently released a new source code scanning tool, CodeScan. CodeScan is an advanced auditing tool designed to check web application source code for security vulnerabilities.

CodeScan utilises an intelligent source code parsing engine, traversing execution paths and tracking the flow of user supplied input.

During the beta testing of CodeScan PHP, the Avatar MOD v1.3 for Snitz Forums was selected as a test case application.

This advisory is the result of research into the security of the Avatar MOD v1.3 for Snitz Forums, based on the report generated by the CodeScan tool.

== Vulnerability Details ==

* Arbitrary File Upload *

The Avatar MOD gives portal administrators the ability to upload avatar images to be used within the forum. CodeScan located a file upload vulnerability in the avatar_upload.asp which can be exploited by a remote user to upload any arbitrary file.

[Start Pseudo Code]

```
Dim arrAllowedTypes : arrAllowedTypes = Array(".jpg", ".jpeg", ".gif", ".png")
Dim strExtension : strExtension = LCase(Mid(FileName, InStrRev(FileName, ".")))
Dim intForCounter
Dim blnAllow : blnAllow = False

for intForCounter = 0 to Ubound(arrAllowedTypes)
  if strComp(strExtension, arrAllowedTypes(intForCounter), 1) = 0 then blnAllow = True
next


if Not blnAllow then
  UploadMessage = "Failed - File type [" & strExtension & "] is not allowed."
  Exit Sub
End if
```

[End Pseudo Code]

This function is vulnerable to the ASP Null Byte problem as documented in http://www.security-assessment.com/Whitepapers/0x00_vs_ASP_File_Uploads.pdf

Exploitation occurs when a null byte is embedded in the filename sent with the upload. If a user were to upload the file test.asp[NULLBYTE].jpg the application will write the file test.asp file to a writeable directory inside the web root.

== Solutions ==



"Hamiln" the developer of the Avatar MOD was contacted in early April, and we did not receive any response. Security-Assessment.com recommends the file avatar_upload.asp be removed from any production web servers until a new version of the software is released.

== Credit ==

Discovered by Paul Craig of Security-Assessment.com

MORE INFORMATION

- » [CodeScan Overview](#)
- » [CodeScan Features](#)
- » [Technical Support Info](#)

NEXT STEPS

Every organisations needs and uses for CodeScan vary. [Contact Us](#) to discuss opportunities, benefits and implementation of CodeScan.

[CodeScan.com](#) © 2005 | [Privacy Policy](#) | [Terms Of Use](#) | [Site Map](#)