

[NT] GameSpy Arcade Arbitrary File Writing

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-07/0130.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 07/31/03

To: list@securiteam.com

Date: 31 Jul 2003 14:09:41 +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

Get Thawte's New Step-by-Step SSL Guide for Apache.

In this guide you will find out how to test, purchase, install and use a Thawte Digital Certificate on you Apache web server. Throughout, best practices for set-up are highlighted to help you ensure efficient ongoing management of your encryption keys and digital certificates. Get you copy of this new guide now: <http://ad.doubleclick.net/clk;5903117;8265118;i>

GameSpy Arcade Arbitrary File Writing

SUMMARY

The problem exists within GSAPAK.EXE, a game update agent that is included by default with the installation of GameSpy Arcade.

GameSpy automatically adds three mime types to the list of accepted documents in Internet Explorer and Netscape Navigator, which are:

"application/x-gsarcade-usersvc"

"application/x-gsarcade-skinpak"

"application/x-gsarcade-launch"

By default, when a file with the extension of .APK, .arcade or .asn is received, it will be launched by GSAPAK.exe. Due to insufficient checks on files being handled by the GameSpy update engine, it is possible by an attacker to construct a special ZIP that will contain files that will overwrite critical files (residing under directories other than those used by GameSpy).

DETAILS

Securiteam: [NT] GameSpy Arcade Arbitrary File Writing

When a user receives a file with the .APK extension, it is actually a simple ZIP file. An attacker could simply construct a ZIP file, and change the path so that it would be extracted into the root directory of the drive, or even the startup directory of Windows.

Utilizing this method will allow attackers to insert a virus, Trojan horse, or pretty much anything one desires, into the victim's system.

i.e.: ../.././calc.exe – Would put it in the root directory

Because the file is considered an accepted type by browsers, there will be no dialog asking the user to accept or deny receiving it.

Risk:

If a user were to have JavaScript enabled, the attacker could even add "onLoad=" to an IMG tag on a web page, which would run the file upon the image being loaded. This could have serious consequences on Gaming Forums.

This bug does not require GameSpy Arcade to be running in the background, as simply having it installed would suffice. It is possible that it has been installed along with a game, and has not been touched. This does not make the user safe. GSAPAK.exe is a separate entity in the GameSpy package, and is useful for the purpose they have created it.

Fix:

GameSpy was notified on July 28, 2003.

GameSpy responded very quickly, and they were on their way to fixing the bug within 12 hours of the initial contact.

Directory of GameSpy Technology, David Wright, has told TZT that this vulnerability will be fixed in a patch this week. We would like to thank GameSpy for their extremely fast response and professionalism in handling this matter.

Current GameSpy Arcade users should see the patch, and be given the option (possibly required) to update. We suggest the latter.

If you have concerns about waiting for the patch, it can be temporarily fixed by removing the above-specified accepted documents from the registry. You could also remove GSAPAK.exe, or you could even choose to uninstall GameSpy Arcade until the patch becomes available later this week.

ADDITIONAL INFORMATION

The information has been provided by <mailto:zzz@threezee.com> Mike Kristovich.

=====

Securiteam: [NT] GameSpy Arcade Arbitrary File Writing

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.