

[NT] DivX Player Skin Directory Traversal

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-01/0093.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 01/23/05

To: list@securiteam.com

Date: 23 Jan 2005 14:30:07 +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>

DivX Player Skin Directory Traversal

SUMMARY

As the name suggests, <<http://www.divx.com/divx/player/>> DivX Player is "a Windows player for DivX files. It is included by default in the DivX codec distributed by DivXNetworks".

Due to improper filtering by the DivX Player skin installer, an attacker can cause DivX Player to overwrite arbitrary files by utilizing a directory traversal vulnerability.

DETAILS

Vulnerable Systems:

* DivX Player version 2.6 and prior

The skins used by DivX Player are actually zip files containing all the needed images and a script file. When the player loads a skin, it unpacks the skin in the temporary system directory into a folder named with the DPS's name.

An attacker can overwrite the files on the victim's disk in that is located the temporary folder (usually c:) using the classical directory traversal path like:

Securiteam: [NT] DivX Player Skin Directory Traversal

..\..\..\windows\notepad.exe

Can be used both slash and backslash.

Proof of concept:

A proof of concept can be downloaded from:

<<http://alugi.altervista.org/poc/divxplayerbug.dps>>

<http://alugi.altervista.org/poc/divxplayerbug.dps>

ADDITIONAL INFORMATION

The information has been provided by <<mailto:alugi@autistici.org>> Luigi Auriemma.

The original article can be found at:

<<http://alugi.altervista.org/adv/divxplayer-adv.txt>>

<http://alugi.altervista.org/adv/divxplayer-adv.txt>

=====

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.