

# [NT] Multiple Vulnerabilities in PY Software Active Webcam WebServer

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-03/0041.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 03/10/05

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 10 Mar 2005 17:21:59 +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>

-----

Multiple Vulnerabilities in PY Software Active Webcam WebServer

---

## SUMMARY

" <<http://www.pysoft.com/ActiveWebCamMainpage.htm>> Active WebCam captures images up to 30 frames per second from any video device including USB, analog cameras, TV-boards, camcorders, and from network IP cameras. The program performs simultaneous recording and broadcasting from unlimited number of cameras."

There are multiple vulnerabilities founded in PYSoftware Active Webcam WebServer, including Denial of Service and Information Disclosure.

## DETAILS

Vulnerable Systems:

\* PY Software Active Webcam version 5.5

Floppy Disk Request Denial of Service:

<http://example.net:8080/A:\a.txt>

This request will force the webcam.exe to access the A:\a.txt, And if there is no floppy disk in the A: drive, the system will pop up a message like "There is no disk in the drive. Please insert a disk into drive A:".

## Securiteam: [NT] Multiple Vulnerabilities in PY Software Active Webcam WebServer

Before the administrator press "Cancel" or "Yes", the other request will be paused, that means the other user cannot access the HTTP Server, thus leading to a Denial Of Service.

Filelist.html Denial of Service:

<http://example.net:8080/Filelist.html>

When requesting the filelist.html, the target's CPU usage will be 100%, and it seems that Explorer.exe use 95%.

Physical Path Disclosure:

<http://example.net:8080/a>

The Server will return "The requested file: C:\Program Files\Active WebCam\images\a\ was not found."

File Disclosure:

The HTTP server returns the different result between an existed file and a not existed file.

<http://example.net:8080/c:\nonexsit.txt>

the HTTP Server returns "Active WebCam cannot find this file"

<http://example.net:8080/c:\boot.ini>

the HTTP Server returns "HTTP 403 Forbidden"

Thus leading to System information disclosure, and can be used to verify whether some particular software is installed, for example:

<http://example.net:8080/C:\Snort\bin\snort.exe>

will disclosure whether a snort is installed on the server, and give additional information to the attacker.

Memory Exhaust Denial of service:

It seems that WebCam HTTP server cannot correctly release the memory and thus lead to a denial of service. Simply connect() and send() a HTTP request, webcam.exe will eat at least 52k memory, and send the HTTP request thousands times, the system will encounter a Memory exhaust. The webcam.exe will crash, or the http server will automatically restart. The following information will be logged in System Event Log, "Access violation at address (...) in module 'WebCam.exe'. Write of address (...).", "Invalid pointer operation."

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:smaillist@gmail.com>> Sowhat.

The original article can be found at:

<<http://secway.org/advisory/ad20050104.txt>>

<http://secway.org/advisory/ad20050104.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](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto:list-subscribe@securiteam.com)

Securiteam: [NT] Multiple Vulnerabilities in PY Software Active Webcam WebServer

=====  
=====

**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.