

# [NT] AntiVirus Filename Bypassing

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-09/0105.html>

---

**From:** SecuriTeam (*support\_at\_securiteam.com*)

**Date:** 09/29/05

To: list@securiteam.com

Date: 29 Sep 2005 10:43:46 +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>

-----

AntiVirus Filename Bypassing

---

## SUMMARY

Several AntiVirus programs do not scan filenames that contain non-printable ASCII characters, in addition instead of blocking them they are simply ignored.

## DETAILS

### Vulnerable Systems:

- \* BitDefender Antivirus
- \* Trustix Antivirus
- \* Avast! Antivirus
- \* Cat Quick Heal Antivirus
- \* Abacre Antivirus
- \* VisNetic Antivirus (bypass only with manual scan)
- \* AntiVir Personal Edition Antivirus
- \* Clamav for Windows Antivirus
- \* Lavasoft Adware SE Personal Edition
- \* Antiy Ghostbusters Professional Edition

### Immune Systems:

- \* Kaspersky Antivirus
- \* AVG Free

## Securiteam: [NT] AntiVirus Filename Bypassing

Several AntiVirus programs do not scan files that contain extended ASCII characters and characters that are lower than 0x20. An attacker can rename a malicious filename to such a filename which in turn will cause the AntiVirus programs to ignore the filename.

Proof of Concept:

If your Antivirus options are:

- "Scan on accessed files"
- "A real time protection"

If you want to test this PoC, don't forget to temporarily disabling before handling!

Select only a "detected" program that does not have to disturb the correct operation of your machine!

Find a program detected by your software protection.  
BitDefender for example don't like ClearLogs.

ClearLogs clears the local or remote event log computer.

Ref: <http://ntsecurity.nu/downloads/clearlogs.exe>

BitDefender >> Detected: Application.Clearlog.A

Rename clearlogs.exe to clearlogs[Here press Alt + 1].exe  
Alt + "some numbers" generate specials ASCII characters.

Ref: <http://www.lookuptables.com>

After that re-activate the real time protection.

Then if you scan it ...

[100%] "Scan successful: no viruses found"

Open your CMD and execute.

X:\SecuBox.Labs\clearlogs ~ .exe

ClearLogs 1.0 - (c) 2002, Arne Vidstrom

Usage: clearlogs [\\computername] <-app / -sec / -sys>

-app = application log

-sec = security log

-sys = system log

If we take a look to [Show report] - Statistics

Scan path: X:\SecuBox.Labs\clearlogs?.exe

Folders: 0

Files: 4

Archives: 0

Packed files: 0

Identified viruses: 0

Infected files: 0

Warnings: 0

Suspect files: 0

Disinfected files: 0

Deleted files: 0

Securiteam: [NT] AntiVirus Filename Bypassing

Copied files: 0  
Moved files: 0  
Renamed files: 0  
I/O errors: 0  
Scan time: 00:00:01  
Scan speed (files/sec): 4

ADDITIONAL INFORMATION

The information has been provided by <<mailto:unsecure@writeme.com>>  
SecuBox Labs.

=====

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)

=====  
=====

**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.