

[NEWS] Multiple Antivirus Malformed Filename Bypassing

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-03/0105.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 03/23/05

To: list@securiteam.com

Date: 23 Mar 2005 10:23:29 +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 Antivirus Malformed Filename Bypassing

SUMMARY

Escape sequences in filenames contained in ZIP archives do not get escaped whenever they are displayed or logged, allowing a remote attacker to cause the Antiviruses scanning engine to skip their scanning.

DETAILS

Many Antivirus software products log filenames during decompressing, so that they can then have a list of all the files they need to test (usually by using Perl Archive::Zip module). This allows an attacker to create special filenames inside compressed file that would evade the Antivirus's processing of the list allowing them to travel unchecked.

Proof of Concept

```
eicar_com &#9835; .&#9786;&#9787;&#9829;&#9830;&#9827;&#9824;*&#9688;  
'&#8596;&#9650; .com .zip
```

The testing was made with 4 type of files:

*

<<ftp://ftp.aerasec.de/pub/advisories/unfiltered-escape-sequences/no-escape-sequences-in-filename-eicar.zip>>

Securiteam: [NEWS] Multiple Antivirus Malformed Filename Bypassing

unfiltered-escape-sequences/no-escape-sequences-in-filename-eicar.zip

*

<<ftp://ftp.aerasesc.de/pub/advisories/unfiltered-escape-sequences/no-escape-sequences-in-filename-sober.l.zip>>

no-escape-sequences-in-filename-sober.l.zip

*

<<ftp://ftp.aerasesc.de/pub/advisories/unfiltered-escape-sequences/unfiltered-escape-sequences-in-filename-eicar.zip>>

unfiltered-escape-sequences-in-filename-eicar.zip

*

<<ftp://ftp.aerasesc.de/pub/advisories/unfiltered-escape-sequences/unfiltered-escape-sequences-in-filename-sober.l.zip>>

unfiltered-escape-sequences-in-filename-sober.l.zip

Testing Result:

From <ftp://ftp.aerasesc.de/pub/advisories/unfiltered-escape-sequences/>

File unfiltered-escape-sequences-in-filename-eicar.zip

AntiVir : Eicar-Test-Signature

Avast : EICAR Test-NOT!!

AVG Antivirus : No viruses found

BitDefender : EICAR-Test-File (not a virus) (0.52 seconds taken)

ClamAV : Eicar-Test-Signature (0.59 seconds taken)

Dr.Web : EICAR Test File (NOT a Virus!) (0.90 seconds taken)

F-Prot Antivirus : EICAR_Test_File (0.29 seconds taken)

Fortinet : EICAR_TEST_FILE (1.20 seconds taken)

Kaspersky Anti-Virus : EICAR-Test-File (3.04 seconds taken)

mks_vir : Eicar.Test (probable variant) (0.70 seconds taken)

NOD32 : Eicar test file (1.55 seconds taken)

Norman Virus Control : EICAR_Test_file_not_a_virus! (0.48 seconds taken)

Result: AVG fails.

From <ftp://ftp.aerasesc.de/pub/advisories/unfiltered-escape-sequences/>

File unfiltered-escape-sequences-in-filename-sober.l.zip

AntiVir : Worm/Sober.L (0.42 seconds taken)

Avast : Win32:Sober-K (1.53 seconds taken)

AVG Antivirus : No viruses found (0.52 seconds taken)

BitDefender : Win32.Sober.L@mm (0.53 seconds taken)

ClamAV : Worm.Sober.L (0.60 seconds taken)

Dr.Web : Win32.HLLM.Generic.328 (0.94 seconds taken)

F-Prot Antivirus : W32/Sober.M@mm (0.09 seconds taken)

Fortinet : W32/Sober.M-mm (0.45 seconds taken)

Kaspersky Anti-Virus : Email-Worm.Win32.Sober.l (1.03 seconds taken)

mks_vir : Worm.Sober.L (0.24 seconds taken)

NOD32 : Win32/Sober.L (0.48 seconds taken)

Norman Virus Control : Sober.L@mm (0.18 seconds taken)

Result: AVG fails.

From <ftp://ftp.aerasesc.de/pub/advisories/unfiltered-escape-sequences/>

File no-escape-sequences-in-filename-eicar.zip

Securiteam: [NEWS] Multiple Antivirus Malformed Filename Bypassing

AntiVir : Eicar-Test-Signature (0.38 seconds taken)
Avast : EICAR Test-NOT!! (1.52 seconds taken)
AVG Antivirus : EICAR_Test (0.52 seconds taken)
BitDefender : EICAR-Test-File (not a virus) (0.52 seconds taken)
ClamAV : Eicar-Test-Signature (0.59 seconds taken)
Dr.Web : EICAR Test File (NOT a Virus!) (0.90 seconds taken)
F-Prot Antivirus : EICAR_Test_File (0.09 seconds taken)
Fortinet : EICAR_TEST_FILE (0.45 seconds taken)
Kaspersky Anti-Virus : EICAR-Test-File (1.00 seconds taken)
mks_vir : Eicar.Test (probable variant) (0.23 seconds taken)
NOD32 : Eicar test file (0.47 seconds taken)
Norman Virus Control : EICAR_Test_file_not_a_virus! (0.18 seconds taken)

Results: No failures.

From <ftp://ftp.aerasesc.de/pub/advisories/unfiltered-escape-sequences/>
File no-escape-sequences-in-filename-sober.l.zip

Short version : Results: No failures.

visitbipin@yahoo.com posted this POC (over FD)
http://www.geocities.com/visitbipin/test_nav.zip

AntiVir : Eicar-Test-Signature
Avast : EICAR Test-NOT!!
AVG Antivirus : EICAR_Test
BitDefender : EICAR-Test-File
ClamAV : No viruses found
Dr.Web : EICAR Test File
F-Prot Antivirus : No viruses found
Fortinet : No viruses found
Kaspersky Anti-Virus : EICAR-Test-File
mks_vir : Eicar.Test (probable variant)
NOD32 : No viruses found
Norman Virus Control : No viruses found

visitbipin@hotmail.com posted this POC
<http://www.geocities.com/visitbipin/gpbf.zip>

AntiVir : No viruses found
Avast : EICAR Test-NOT!!
AVG Antivirus : EICAR_Test
BitDefender : EICAR-Test-File (not a virus)
ClamAV : Eicar-Test-Signature
Dr.Web : EICAR Test File (NOT a Virus!)
F-Prot Antivirus : No viruses found
Fortinet : EICAR_TEST_FILE
Kaspersky Anti-Virus : No viruses found
mks_vir : No viruses found
NOD32 : Eicar test file
Norman Virus Control : No viruses found

Securiteam: [NEWS] Multiple Antivirus Malformed Filename Bypassing

* Some AntiVirus software detect the virus only in second part of the ZIP file, so it looks like the first one is really skipped and not analysed.

* ClamAV act a bit different then the rest of the AntiViruses. When it locate one virus inside a ZIP file, it does not continue to scan the rest of the files inside, and it display the amount of files scanned without including the files inside the ZIP file itself.

Disclosure Timeline:

2005-03-09: Initial version

2005-03-10: Minor update, add results of clamav, Trend Micro, Sophos

2005-03-14: Update status and results, add result of WebWasher

2005-03-15: Add an additional URL

2005-03-15a: Update result on Sophos (additional command line switch helps) minor fixes

2005-03-16: Add URL to Thierry Zoller posting, note here that AVG AV fails add result of Trend Micro IMSS (it's ok)

2005-03-17: Add additional URLs

2005-03-18: WebWasher notified us about a new fixed version

ADDITIONAL INFORMATION

The information has been provided by <mailto:pbieringer@aerasec.de> Dr. Peter Bieringer.

The original article can be found at:

<<ftp://ftp.aerasec.de/pub/advisories/unfiltered-escape-sequences/unfiltered-escape-sequences.txt>>
unfiltered-escape-sequences.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.