

Re: Unfiltered escape sequences in filenames contained in ZIP archives wouldn't be escaped on displaying or logging, and

# [Full-disclosure] Re: Unfiltered escape sequences in filenames contained in ZIP archives wouldn't be escaped on displaying or logging, and can also lead to bypass AV scanning

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2005-03/0557.html>

---

**From:** Thierry Zoller (*Thierry\_at\_sniff-em.com*)

**Date:** 03/15/05

Date: Tue, 15 Mar 2005 22:42:39 +0100

To: "Dr. Peter Bieringer" <pbieringer@aerasec.de>

Dear List,

Updated: State as of 15/03/2005

From <ftp://ftp.aerasec.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.aerasec.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)

[Full-disclosure] Re: Unfiltered escape sequences in filenames contained in ZIP archives wouldn't be escaped

[Full-disclosure] Re: Unfiltered escape sequences in filenames contained in ZIP archives wouldn't be escaped on displaying or logging, and

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.aerasesec.de/pub/advisories/unfiltered-escape-sequences/>  
File no-escape-sequences-in-filename-eicar.zip

---

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.aerasesec.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](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

[Full-disclosure] Re: Unfiltered escape sequences in filenames contained in ZIP archives wouldn't be escaped

[Re: Unfiltered escape sequences in filenames contained in ZIP archives wouldn't be escaped on displaying or logging, and

<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

---

Results: Archives modified by visitbipin@hotmail.com fail on more scanners. Why, I ignore.

--

Thierry Zoller  
mailto:Thierry@sniff-em.com

---

Full-Disclosure - We believe in it.  
Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>  
Hosted and sponsored by Secunia - <http://www.secunia.com/>

[Full-disclosure] Re: Unfiltered escape sequences in filenames contained in ZIP archives wouldn't be escaped