F-Prot/Frisk Anti Virus bypass - ZIP Version Header

Ref   : TZO-012005-Fprot
Author : Thierry Zoller / Security Engineer
WWW   : http://thierry.sniff-em.com
Article : http://thierry.sniff-em.com/research/fprot.html

I. Background

http://www.f-prot.com/products/corporate_users/

FRISK Software International has, since it was first established in 1993, consistently maintained its position as one of the world's leading companies in antivirus research and product development.

FRISK Software produces the hugely popular F-Prot Antivirus products range offering unrivalled neural network and heuristic detection capabilities. In addition to this, the F-Prot AVES managed online e-mail security service filters away the nuisance of spam e-mail as well as viruses, worms and other malware that increasingly clog up inboxes and threaten data security.

F-Prot Antivirus for Windows
F-Prot Antivirus for Microsoft Exchange
F-Prot Antivirus for Linux x86 / BSD x86
F-Prot Antivirus for AIX
F-Prot Antivirus for DOS
F-Prot Antivirus for Solaris SPARC / Solaris x86
F-Prot Antivirus for AIX

II. Description

The F-prot engines failes to decompress ZIP files which have a version header greater then 15. The consequence is that the F-prot Engine is unable to scan the virus/malware inside and consequently flags it as harmless. If used as an Email Gateway solution the offending Emails will slip through.

```
Local ZIP file header:
local file header signature     4 bytes  (0x04034b50)
version needed to extract       2 bytes
```

Winzip, Winrar, MS Zip engine decompress fine.

```
Tested offset :
Offset       0  1  2  3  4  5  6  7   8  9 10 11 12 13 14 15
00000000   50 4B 03 04 15 00 00 00  00 00 88 80 38 33 3C CF
00000016   51 68 44 00 00 00 44 00  00 00 09 00 00 00 65 69
```

In this example byte 4 has the version header value 15. F-prot fails to decompress the ZIP files with a version header greater then 15.

Solution:
The ZIP decompression engine should ignore the Version header of the ZIP file and nonetheless decompress the file whatever the version field indicates.

III. Summary

Vendor contact : 30/10/2005
Vendor Response : 01/11/2005

> Thank you very much for notifying us of this bug in the current version of F-Prot Antivirus. A fix for this bug will be included in future versions of F-Prot Antivirus.

IV. Thanks

http://virusscan.jotti.org/
http://www.virustotal.com

```
#      : TZO-012005-Fprot
Author : Thierry Zoller / Security Engineer
WWW    : http://thierry.sniff-em.com
```