

[NEWS] F-Prot/Frisk Antivirus ZIP Version Header Bypass

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-11/0042.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 11/10/05

To: list@securiteam.com

Date: 10 Nov 2005 14:59:23 +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>

F-Prot/Frisk Antivirus ZIP Version Header Bypass

SUMMARY

" <http://www.f-prot.com/products/corporate_users/> FRISK Software produces the hugely popular F-Prot Antivirus products range offering unrivaled neural network and heuristic detection capabilities."

F-Prot Antivirus does not recognize ZIP header with length bigger the 15, allowing viruses to bypass the virus scanning techniques used by the product.

DETAILS

Vulnerable Systems:

- * 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

Securiteam: [NEWS] F-Prot/Frisk Antivirus ZIP Version Header Bypass

The F-prot engines fails to decompress ZIP files that 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.

Vendor Response:

"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."

Disclosure Timeline:

Vendor contact : 30/10/2005

Vendor Response : 01/11/2005

ADDITIONAL INFORMATION

The information has been provided by <mailto:Thierry@sniff-em.com>
Thierry Zoller.

The original article can be found at:

<<http://thierry.sniff-em.com/research/fprot.html>>
<http://thierry.sniff-em.com/research/fprot.html>

=====

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.