

[NEWS] F-Secure Multiple Products ARJ Archive Handling Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-02/0061.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 02/15/05

To: list@securiteam.com

Date: 15 Feb 2005 14:10:41 +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-Secure Multiple Products ARJ Archive Handling Vulnerability

SUMMARY

The F-Secure AntiVirus Library is "widely relied upon to provide AntiVirus capabilities to desktop, server, and gateway systems".

ISS X-Force has reported a vulnerability in multiple F-Secure products, which can be exploited by malicious people to compromise a vulnerable system by crafting an archive file, an attacker is able to trigger a heap overflow within the process importing the F-Secure AntiVirus Library.

DETAILS

Vulnerable Systems:

- * F-Secure Anti-Virus for Workstation version 5.43 and earlier
- * F-Secure Anti-Virus for Windows Servers version 5.50 and earlier
- * F-Secure Anti-Virus for Citrix Servers version 5.50
- * F-Secure Anti-Virus for MIMESweeper version 5.51 and earlier
- * F-Secure Anti-Virus Client Security version 5.55 and earlier
- * F-Secure Anti-Virus for MS Exchange version 6.31 and earlier
- * F-Secure Internet Gatekeeper version 6.41 and earlier
- * F-Secure Anti-Virus for Firewalls version 6.20 and earlier

Securiteam: [NEWS] F-Secure Multiple Products ARJ Archive Handling Vulnerability

- * F-Secure Internet Security 2004 and 2005
- * F-Secure Anti-Virus 2004 and 2005
- * Solutions based on F-Secure Personal Express version 5.10 and earlier
- * F-Secure Anti-Virus for Linux Workstations version 4.52 and earlier
- * F-Secure Anti-Virus for Linux Servers version 4.61 and earlier
- * F-Secure Anti-Virus for Linux Gateways version 4.61 and earlier
- * F-Secure Anti-Virus for Samba Servers version 4.60
- * F-Secure Anti-Virus Linux Client Security 5.01 and earlier
- * F-Secure Anti-Virus Linux Server Security 5.01 and earlier
- * F-Secure Internet Gatekeeper for Linux 2.06

Description:

The vulnerability is caused due to a boundary error in the AntiVirus scanning functionality when processing ARJ archives. This can be exploited to cause a buffer overflow via a specially crafted ARJ archive.

Successful exploitation allows execution of arbitrary code, but requires that the malicious ARJ archive is scanned with archive scanning enabled.

Solution:

Apply patches listed in F-Secure's advisory:

<<http://www.f-secure.com/security/fsc-2005-1.shtml>>
<http://www.f-secure.com/security/fsc-2005-1.shtml>.

ADDITIONAL INFORMATION

The information has been provided by <mailto:papp_geza1@axelero.hu> Geza Papp dr (Axelero).

=====

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.