

n.runs AG
<http://www.nruns.com/>
n.runs-SA-2007.014

[security\(at\)nruns.com](mailto:security(at)nruns.com)
04-Jun-2007

Vendor: F-Secure Corporation, <http://www.f-secure.com>

Affected Products:

F-Secure Anti-Virus for Workstations version 7.00 and earlier
F-Secure Anti-Virus for Windows Servers version 7.00 and earlier
F-Secure Anti-Virus for Citrix Servers version 5.52
F-Secure Anti-Virus for MIMESweeper version 5.61 and earlier
F-Secure Anti-Virus Client Security version 7.00 and earlier
F-Secure Anti-Virus for MS Exchange version 7.00 and earlier
F-Secure Internet Gatekeeper version 6.60 and earlier
F-Secure Internet Security 2005, 2006 and 2007
F-Secure Anti-Virus 2005, 2006 and 2007
Solutions based on F-Secure Protection Service for Consumers
version 7.00 and earlier
F-Secure Anti-Virus for Linux Servers version 4.65 and earlier
F-Secure Anti-Virus for Linux Gateways version 4.65 and earlier
F-Secure Anti-Virus Linux Client Security 5.52 and earlier
F-Secure Anti-Virus Linux Server Security 5.52 and earlier
F-Secure Internet Gatekeeper for Linux 2.16 and earlier

Vulnerability: Infinite Loop DoS (remote)

Risk: HIGH

Vendor communication:

2007/05/07	initial notification to F-Secure Corporation
2007/05/08	F-Secure Corporation Response
2007/05/08	PGP public keys exchange
2007/05/08	PoC files sent to F-Secure Corporation
2007/05/14	F-Secure Corporation acknowledged the PoC files
2007/05/18	F-Secure Corporation validate the Vulnerability
2007/05/18	F-Secure Corporation notify update release date
2007/05/30	F-Secure Corporation released Update with fixes

Overview:

F-Secure Corporation protects consumers and businesses against computer viruses and other threats from the Internet and mobile networks.

F-Secure award-winning solutions are available for workstations, gateways, servers and mobile phones. They include antivirus and desktop firewall with intrusion prevention, antispam and antispysware solutions, as well as network control solutions for Internet Service Providers.

F-Secure protection is also available as a service through major ISPs, such as France Telecom, TeliaSonera, PCCW and Charter Communications. F-Secure is the global market leader in mobile phone protection provided through mobile operators, such as T-Mobile and Swisscom and mobile handset manufacturers such as Nokia.

Description:

A remotely exploitable vulnerability has been found in the files parsing engine.

In detail, the following flaw was determined:

- Infinite Loop in .ARJ files parsing

Impact:

This problem can lead to remote denial of service provoked by high CPU consume and exhaustion of storage resource if an attacker carefully crafts a file that exploits the aforementioned vulnerability. The vulnerability is present in F-Secure Corporation software products above mentioned in all platforms supported by the affected products.

Solution:

The vulnerability was reported on 07.May.2007 and an update has been issued on 30.May.2007 to solve this vulnerability. For detailed information about the fixes follow the link in References [1] section of this document.

Credit:

Bugs found by Sergio Alvarez of n.runs AG.

References:

<http://www.f-secure.com/security/fsc-2007-3.shtml> [1]

This Advisory and Upcoming Advisories:

http://www.nruns.com/security_advisory.php

Unaltered electronic reproduction of this advisory is permitted. For all other reproduction or publication, in printing or otherwise, contact security@nruns.com for permission. Use of the advisory constitutes acceptance for use in an "as is" condition. All warranties are excluded. In no event shall n.runs be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages, even if n.runs has been advised of the possibility of such damages.

Copyright 2007 n.runs AG. All rights reserved. Terms of apply.