

# [VulnWatch] SRT2004-01-9-1022 – Symantec LiveUpdate allows local users to become SYSTEM

*Source:* <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2004-01/0010.html>

---

*From:* KF ([dotslash\\_at\\_snosoft.com](mailto:dotslash_at_snosoft.com))

*Date:* 01/12/04

Date: Mon, 12 Jan 2004 07:22:39 -0500

To: [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)

As usual full details are available at <http://www.secnetops.biz/research>

-KF

Secure Network Operations, Inc. <http://www.secnetops.com/research>

Strategic Reconnaissance Team [research\[at\]secnetops\[.\]com](mailto:research[at]secnetops[.]com)

Team Lead Contact [kf\[at\]secnetops\[.\]com](mailto:kf[at]secnetops[.]com)

Spam Contact `rm -rf ^@snosoft.com`

## Our Mission:

\*\*\*\*\*

Secure Network Operations offers expertise in Networking, Intrusion Detection Systems (IDS), Software Security Validation, and Corporate/Private Network Security. Our mission is to facilitate a secure and reliable Internet and inter-enterprise communications infrastructure through the products and services we offer.

To learn more about our company, products and services or to request a demo of ANVIL FCS please visit our site at <http://www.secnetops.com>, or call us at: 978-263-3829

## Quick Summary:

\*\*\*\*\*

Advisory Number : SRT2004-01-09-1022

Product : Symantec LiveUpdate

Version : 1.70.x through 1.90.x

Vendor : <http://symantec.com/techsupp/files/lu/lu.html>

Class : Local

Criticality : High (to users of the below listed products)

Products Affected : Symantec LiveUpdate 1.70.x through 1.90.x

: Norton SystemWorks 2001-2004

: Norton AntiVirus (and Pro) 2001-2004

: Norton Internet Security (and Pro) 2001-2004

VulnWatch: [VulnWatch] SRT2004-01-9-1022 – Symantec LiveUpdate allows local users to become SYSTEM

: Symantec AntiVirus for Handhelds v3.0

Operating System(s) : Win32

Notice

\*\*\*\*\*

The full technical details of this vulnerability can be found at:

<http://www.secnetops.com> under the research section.

Basic Explanation

\*\*\*\*\*

High Level Description : LiveUpdate allows local users to become SYSTEM

What to do : run LiveUpdate and apply latest patches.

Basic Technical Details

\*\*\*\*\*

Proof Of Concept Status : SNO has proof of concept.

Low Level Description : Symantec, the world leader in Internet security technology, provides a broad range of content and network security software and appliance solutions to individuals, enterprises and service providers. The company is a leading provider of client, gateway and server security solutions for virus protection, firewall and virtual private network, vulnerability management, intrusion detection, Internet content and email filtering, and remote management technologies and security services to enterprises and service providers around the world. Symantec's Norton brand of consumer security products is a leader in worldwide retail sales and industry awards. Headquartered in Cupertino, Calif., Symantec has worldwide operations in 36 countries.

Symantec's Norton Internet Security 2004 provides essential protection from viruses, hackers, and privacy threats. During an audit of NIS2004 we uncovered a local privilege escalation issue in LiveUpdate. This issue is similar to the issues that were uncovered in the Windows Help API by both Brett Moore and our SRT team in late 2003.

Full details available at:

<http://www.secnetops.biz/research/SRT2004-01-09-1022.txt> and

<http://www.secnetops.biz/research/SRT2004-01-09-1022.jpg>

Vendor Status : Symantec promptly attended to the issue and was very responsive during all phases of discovery / research and patching. Fixes are now available via LiveUpdate.

Bugtraq URL : To be assigned. CVE candidate CAN-2003-0994.

Disclaimer

---

This advisory was released by Secure Network Operations, Inc. as a matter of notification to help administrators protect their networks against the described vulnerability. Exploit source code is no longer released in our advisories but can be obtained under contract.. Contact our sales department at sales[at]secnetops[.]com for further information on how to

VulnWatch: [VulnWatch] SRT2004-01-9-1022 – Symantec LiveUpdate allows local users to become SYSTEM

obtain proof of concept code.

---

Secure Network Operations, Inc. || <http://www.secnetops.com>

"Embracing the future of technology, protecting you."