

[Full-Disclosure] Happy belated Personal Firewall day – SRT2004-01-17-0628 – Agnitum Optpost firewall allows Local SYSTEM access

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2004-01/0665.html>

From: KF (dotslash_at_snosoft.com)

Date: 01/17/04

To: bugtraq@securityfocus.com

Date: Sat, 17 Jan 2004 14:04:36 -0500

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 : SRT2004-01-17-0628
Product : Outpost Firewall.
Version : 1.x and 2.x
Vendor : <http://www.agnitum.com/download/outpostpro.html>
Class : Local
Criticality : High (to Outpost Firewall users)
Operating System(s) : Win32

Notice

1-2 day Early Warning List:

Secure Network Operations, inc. will very shortly have its own advisory notification mailing list. This list will notify you of advisories 1-2 days in advance of public release to other mailing lists. To subscribe please visit <http://advisories.secnetops.com> in the immediate future.

30-60 day Early Warning List:

Our early warning service will notify you of new vulnerabilities 30-60 days in advance of public release. This service has been created to protect companies by allowing them to repair security vulnerabilities before they become public knowledge. To purchase a one year subscription to this service please contact us at 978-263-3767.

Alert

Our advisories will contain full details excluding a working Proof of Concept. Our web page will contain our working proof of concept for the advisory if it exists. Yes folks this is a policy change for us. We will exercise our own discretion in regards to delay of exploit release vs advisory release. List subscribers will have advanced access to working proof of concept code depending on the severity and list subscription type.

Basic Explanation

High Level Description : Outpost Firewall allows local SYSTEM access.

What to do : Apply update from vendor or limit local access.

Basic Technical Details

Proof Of Concept Status : SNO has Proof of Concept.

Low Level Description : In the words of agnitem... "With hacker attacks and data theft rampant on the Internet, you need a constant defense to safeguard your PC. Antivirus protection is not enough! The comprehensive solution for protecting you and your family online is Outpost Personal Firewall Pro, the world's foremost security application.". Outpost will... "Protect your system from hackers, Guard the privacy of your data, Monitor network activity, Maintain and control your privacy on the Web, Remove annoying ads, And more!".

Our testing was done on the demo version of both Outpost 1.0 and 2.0. We took all defaults while installing from OutpostProInstall.exe. No other tweaks to the settings of Outpost were made.

Once started the outpost service provides a tray icon that is available to all users of the system. outpost.exe runs as SYSTEM so this poses an obvious security risk.

If you wish to take local system rights from Agnitum Outpost Firewall do the following steps.

1. right click tray icon...
2. choose "options..."
3. choose application or plug-ins
4. click Add...
5. browse for c:\winnt\system32\cmd.exe and right click on it...choose open.

Now you have a command prompt running as the user SYSTEM.

There is also a similar alternate method...

1. double click tray icon.
2. click Help.
3. click contents.
4. right click help content...
5. choose view source.
6. you now have notepad.exe running as SYSTEM... taking cmd.exe from here is a matter of going to file then open, and duplicating step 5 above.

Proof Of Concept: Live exploit code will be under our research shortly. Thanks to Brett Moore for all the conceptual help... sorry for my dumb questions! See <http://www.secnetops.biz/research/> look for outpost_ex2.exe and outpost_ex2.c We will update our whats new section when the exploit is available.

A screenshot of exploitation can be located at (without registration): <http://www.secnetops.biz/images/SRT2004-01-17-0628.jpg>

Vendor Status : Vendor is has a fix for the issue. A vendor supplied patch should be supplied in the next week or so (of 1/17/2004). "We are glad to inform you that the problem you had reported was solved.", "We plan to release new version in a couple of weeks.", "We strongly recommend that you join the Agnitum News mailing list at www.agnitum.com/news to keep informed of security issues that may affect you, and of new version release."

We (Snosoft) also recommend you sign up for their list... they are very hard to communicate with otherwise. Web forms and long delays were what we encountered.

Bugtraq URL : To be assigned.

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. Release of exploit code is done at our own discretion.

All content of this advisory is property of Secure Network Operations.

Subject: [Full-Disclosure] Happy belated Personal Firewall day – SRT2004-01-17-0628 – Agnitum Optpost firewall allows Local

Secure Network Operations, Inc. || <http://www.secnetops.com>
"Embracing the future of technology, protecting you."

Full-Disclosure – We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>

[Full-Disclosure] Happy belated Personal Firewall day – SRT2004-01-17-0628 – Agnitum Optpost firewall