

Microsoft RASAPI32.DLL

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2002-06/0122.html>

From: Mark Litchfield (mark@ngssoftware.com)

Date: 06/13/02

From: "Mark Litchfield" <mark@ngssoftware.com>

To: <bugtraq@securityfocus.com>

Date: Thu, 13 Jun 2002 14:23:59 -0700

NGSSoftware Insight Security Research Advisory

Name: Buffer Overflow in Microsoft Rasapi32.dll

Systems Affected: WinNT, Win2K, XP, Microsoft Routing And Remote Access Server ("Steelhead")

Severity: High

Category: Buffer Overrun / Privilege Escalation

Vendor URL: <http://www.microsoft.com/>

Author: Mark Litchfield (mark@ngssoftware.com)

Date: 13th June 2002

Advisory number: #NISR13062002

Vendor Notification Details

The VNA for this issue can be found at

<http://www.nextgenss.com/vna/ms-ras.txt>

The elapsed time between notification and fix was seven months.

Description

Rasapi32.dll contains an unchecked buffer, essentially allowing a local user to overflow any executable that has a GUI help feature or connects to the internet.

This can be used to obtain system privileges on a machine that an attacker can interactively

log on to, or to "Trojan" a machine on which they can edit the phone book properties.

Details

Rasapi32.dll ships with all recent Microsoft operating systems, being described

as the "Dial-Up Networking Dynamic Linked Library and a Remote Access API".

The overflow occurs when the code that parses RAS phonebook entries runs; this can occur when a user logs on interactively, or when a user views the

dial-up

connection properties. Specifically, an overly-long 'script name' (stored in the Rasphone.pbk file)

will cause the overflow.

A possible (interactive) exploit scenario would be:

- Log on to the target machine.
- Create a batch file adding your account to the "administrators" group and paste exploit code that will run the batch file into the 'rasphone.pbk' file.
- Log off user.
- When presented with the logon dialog box, select "Log on using dial-up connection".
- At this point an access violation occurs in Winlogon.exe executing your batch file with system privileges.
Depending on how the exploit code is written, the operating system is likely to 'blue screen' at this point.
- After the blue screen, logon with your user name and password to access your system account.

An interesting aspect of this overflow is that it exploits the logon dialog that occurs after the Secure Attention Sequence (Ctrl+Alt+Del), which is designed to prevent other programs or processes from intervening during authentication (that is, to prevent trojan-horse programs from being executed during the authentication process), effectively turning a defence mechanism into a security problem.

Another interesting point is that on our Windows 2000 test platform the overflow string was Unicode, but on our Windows XP and Windows NT test platforms the overflow string was ASCII.

The overflow can also be used to "poison" a machine such that the next time a dial-up connection is used, some exploit code is run. Interestingly, it is possible to exploit the problem using most windows applications, via the "Internet Options" menu item accessible via the help menu. For example, to cause the overrun to occur in Solitaire (SOL.exe), open Solitaire, select help, contents, options, internet options and finally connections.

Fix Information

NGSSoftware alerted Microsoft to these problems in November of last year.

Microsoft's advisory on this

issue can be found at

<http://www.microsoft.com/technet/security/bulletin/MS02-029.asp>

Microsoft's advisory contains patch download information, as well as a

SecurityFocus Bugtraq: Microsoft RASAPI32.DLL

discussion of the issue.

A check for this issue has been added to Typhon II, of which more information is available from the NGSSoftware website, <http://www.ngssoftware.com>.

Further Information

For further information about the scope and effects of buffer overflows, please see

<http://www.ngssoftware.com/papers/ntbufferoverflow.html>

<http://www.ngssoftware.com/papers/bufferoverflowpaper.rtf>

<http://www.ngssoftware.com/papers/unicodebo.pdf>

<http://www.ngssoftware.com/papers/non-stack-bo-windows.pdf>

- **Previous message:** [Alan Cox: "Re: Very large font size crashing X Font Server and Grounding Server to"](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)