

# [Full-disclosure] Microsoft Registry Editor 5.1/XP/2K long string key vulnerability

*Source:* <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2005-08/0808.html>

---

*From:* Igor Franchuk (*sprog\_at\_online.ru*)

*Date:* 08/24/05

Date: Wed, 24 Aug 2005 11:01:11 +0400

To: bugs@securitytracker.com, news@securiteam.com, full-disclosure@lists.grok.org.uk, <vuln@secun

Hello All,

## PRELUDE

/\*

### Registry Element Size Limits

The following are the size limits for the various registry elements.

The maximum size of a key name is 255 characters.

The maximum size of a value name is as follows:

Windows Server 2003 and Windows XP: 16,383 characters

Windows 2000: 260 ANSI characters or 16,383 Unicode characters.

Windows Me/98/95: 255 characters

Long values (more than 2,048 bytes) should be stored as files with the file names stored in the registry.

This helps the registry perform efficiently. The maximum size of a value is as follows:

Available memory.

Windows Me/98/95: 16,300 bytes. There is a 64K limit for the total size of all values of a key.

\*/

## DESCRIPTION

Microsoft Registry Editor for 2K and XP (Regedt32.exe) has a nice design flow that is naturally allows to hide registry information from viewing and editing even from users with administrative access. (really handfull, thanks guys)

## POC

To reproduce the desired behavior:

– run Regedt32.exe

– create a key, let it just be

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Empty

– in this key create any string value with the name exceeding 256 symbols (260 is the max) or just copy–paste:

helloworldhelloworldhelloworldhelloworldhelloworldhelloworldhelloworldhelloworldhelloworldhelloworld

## Full-Disclosure: [Full-disclosure] Microsoft Registry Editor 5.1/XP/2K long string key vulnerability

Press F5 (refresh) and you will see how the key magically disappears.

Now create ANY key within

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Empty  
and press refresh again – it will NOT BE SEEN by regedt32.

### PRACTICE

There is a tremendous implementation field for this behavior.

### TESTED

On XP SP2 Eng, SP1 and 2K RUS. The testing is by no means complete but I hope it is working on all 2K and XP systems. Sorry if it is not.

### SUGGESTED FIX

Make it possible to manage visibility by specifying (\_?\_) (\_\$\_) and (.\_) in the key names.

--

www.rol.ru

Best regards,

Igor

mailto:sprog@online.ru

NOW SOME REALLY SERIOUS STUFF

Q:

What does boot progress mean?

A:

Bugs, they're warming up.

---

Full-Disclosure - We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia - <http://secunia.com/>