

[Full-Disclosure] Microsoft Windows Huge Text Processing Instability

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2004-10/0636.html>

From: Kaveh Mofidi (*Admin_at_SecureTarget.Net*)

Date: 10/17/04

To: <NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM>

Date: Sun, 17 Oct 2004 11:41:23 +0330

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Secure Target Network (Security Advisory October 17, 2004)

Topic: Microsoft Windows Huge Text Processing Instability

Discovery Date: October 14, 2004

Link to Original Advisory: <http://securetarget.net/advisory.htm>

Affected applications and platforms:

Notepad, NotePad2 and MetaPad (Seems like all Text Processing Apps) /

Microsoft Windows (All Versions)

Introduction:

It is not important, the limitation of opening large text file with "notepad" or similar products like NotePad2

(<http://www.flos-freeware.ch>) and MetaPad

(<http://liquidninja.com/metapad/>); the point is just the way these tiny text processing apps open and handle large text files (talking about over the 200MB).

The way they handle huge text files, it is near possible for a fast modern PC to be completely unstable. This Instability may path to process injection because you cannot even kill the processes of these apps and they will remain "up and running" even when you logged off. So, it's possible for a unprivileged user to simply hook to the remaining process of a privilege user and this lead to information disclosure (simply reading the content of the memory before swapping a large file which happens time after time, based on the file size) but may even lead to running privileged tasks based on the app they used for processing text.

Exploit:

It is different to exploit based on the application you choose for text processing; for windows default notepad.exe, it'll be some like a huge DoS but for NotePad2.exe and MetaPad.exe it is possible to doing process injection (information disclosure and/or running

Full-Disclosure: [Full-Disclosure] Microsoft Windows Huge Text Processing Instability

privileged tasks).

Workaround:

The best way to work around this situation is just not to open large text files in windows! or wait a long time for completion of task.

Tested on:

Microsoft Windows XP SP1/SP2/SP2 on Intel P4 2.4 with 1GB of RAM

Feedback:

Kaveh Mofidi

Head of Secure Target Network

<http://SECURETARGET.NET>

-----BEGIN PGP SIGNATURE-----

Version: PGP 8.0.2

iQA/AwUBQXI0AmO1siv41icpEQKOOQCgx/NNYad1GNBZizskyeNoaRHA4WcAoMVY
legdMSdcweVoBm0jbSxPsEaq
=AIzi

-----END PGP SIGNATURE-----

Full-Disclosure – We believe in it.

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