# Όστε τα Windows XP έγιναν Open Source. Τί σημαίνει αυτό;

Γιώργος Μαμιδάκης

# whoami

- Πρωτοετής φοιτητής @ UOM Τμήμα Εφαρμοσμένης Πληροφορικής
- "Ερευνητικά" ενδιαφέροντα: Linux, Ethical Hacking, Programming
- ckrielle.github.io

# ΠΡΟΕΙΔΟΠΟΙΗΣΗ!!!

Δε σας προτείνω να ψάξετε και να ασχοληθείτε με τον πηγαίο κώδικα καθώς τα πνευματικά δικαιώματα ανήκουν εξ'ολοκλήρου στη Microsoft. Δεν ευθύνομαι για ό,τι κάνετε!

# Τί έγινε στις 24 Σεπτεμβρίου ακριβώς;

- Στην ιστοσελίδα 4chan δημοσιεύθηκε ένα torrent link που περιείχε ένα .7z zip που περιείχε το XP service pack one (XPSP1) και το 2003 server (SVR2003)
- Ο δημοσιευτής πρόσθεσε και αυτό το σχόλιο στο post: "It's been going around privately for many years now."
- Στην αρχή επικρατούσε μία δυσπιστία ως προς την εγκυρότητα του leak
- Ωστόσο αφότου άρχισαν άνθρωποι να το κάνουν επιτυχημένα compile σταμάτησε η ταραχή και άρχισε ο ενθουσιασμός!

# Τί έγινε στις 24 Σεπτεμβρίου ακριβώς;

- Το αρχικό leak ήταν μόνο 6 gb, αλλά μετά άνθρωποι το έβαλαν σε ένα torrent που είχε όλα τα microsoft leaks μέχρι τώρα
- Μαζί με leaks των windows 2000, xbox live και διάφορων nt, υπήρχαν και τα κλασσικά bill gates conspiracies
- Όπως θα περίμενε κάποιος βρέθηκαν κυρίως .c, .cpp, και .h αρχεία
- Από τότε οι προγραμματιστές εργάζονται για να το κάνουν καλύτερο (και προσπαθούν να βρουν μασκοτ!)

# Ήταν δυνατός ο ενθουσιασμός

**Anonymous** Thu 24 Sep 2020 18:45:39 No.77889005 Report

Quoted By: >>77889013 >>77889056 >>77889079 >>77889103 >>77891552 >>77891667 >>77893255 >>77893303 >>77893342

>>77879263

Holy shit. If this is real, then:

>You can run photoshop in a free os

>Reactos can transplant itself and grow from this dump

>You can run daws, vsts etc. on a free os

>Wine can learn from all this and jump to greater heights far faster than was thought possible

>all of this without caring for legality of course

>You can preserve the xp gui and windows 95 style gui (cairo) and extend it to new paradigms and programs, ignoring gtk3 cancer

>Infinitely customizable winxp and win95 guis.

>Create games like touhou 8 through the open source d3d8

I hope this is real.

**Anonymous** Fri 25 Sep 2020 04:31:51 No.77896622 Report

Quoted By: >>77896646 >>77896657 >>77896658

Realistically, what are the ramifications of this? Could we be potentially looking at custom builds that could have modern security put into them by a third party, support for more modern direct X, or better support for modern computer components like 4K monitors, NVME drives, etc? Is there anything that can be done with this to improve XP and give it new life?

**Anonymous** Fri 25 Sep 2020 04:34:16 No.77896646 Report

>>77896620

Maybe it was done on purpose to muddify the preservation effort.

>>77896622

>Could we be potentially looking at custom builds that could have modern security put into them by a third party

>support for more modern direct X

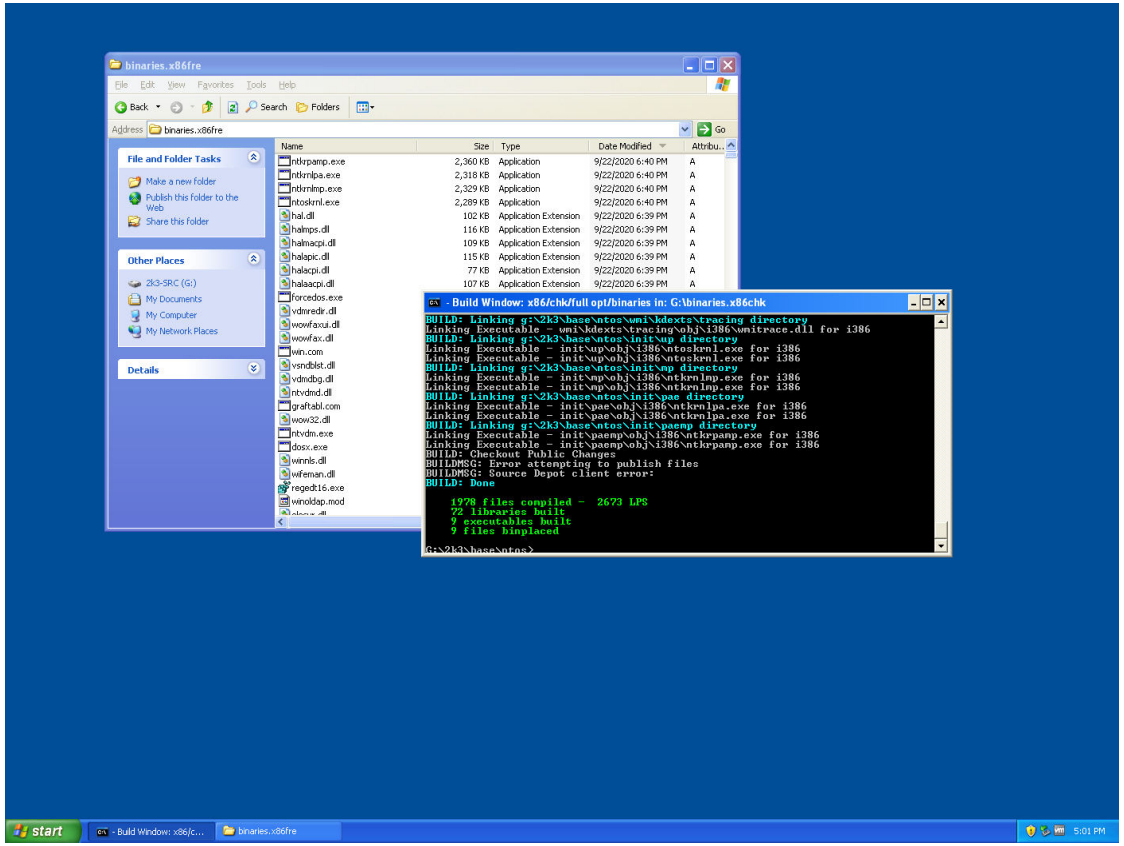
>or better support for modern computer components like 4K monitors, NVME drives, etc?

>Is there anything that can be done with this to improve XP and give it new life?

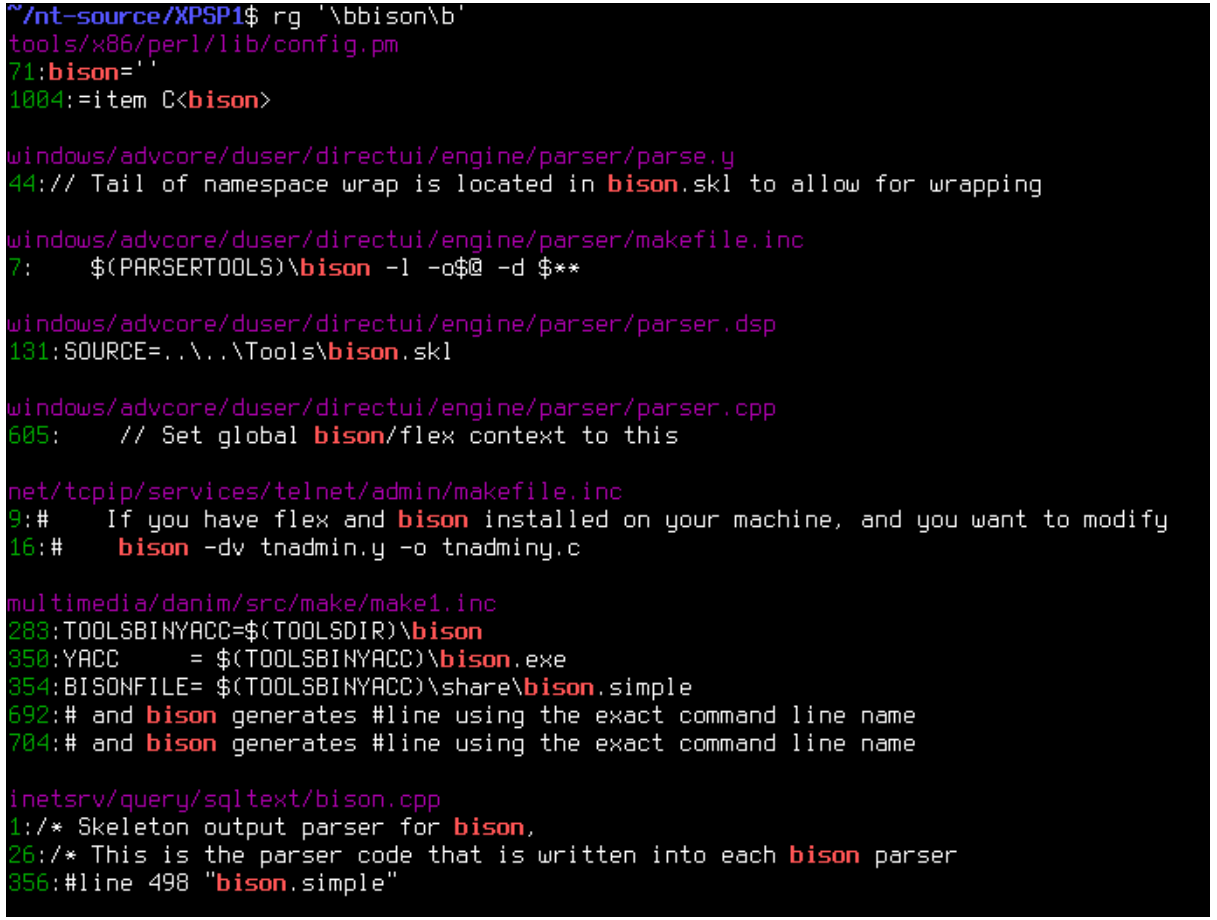
Yes, plenty. All of it in fact.

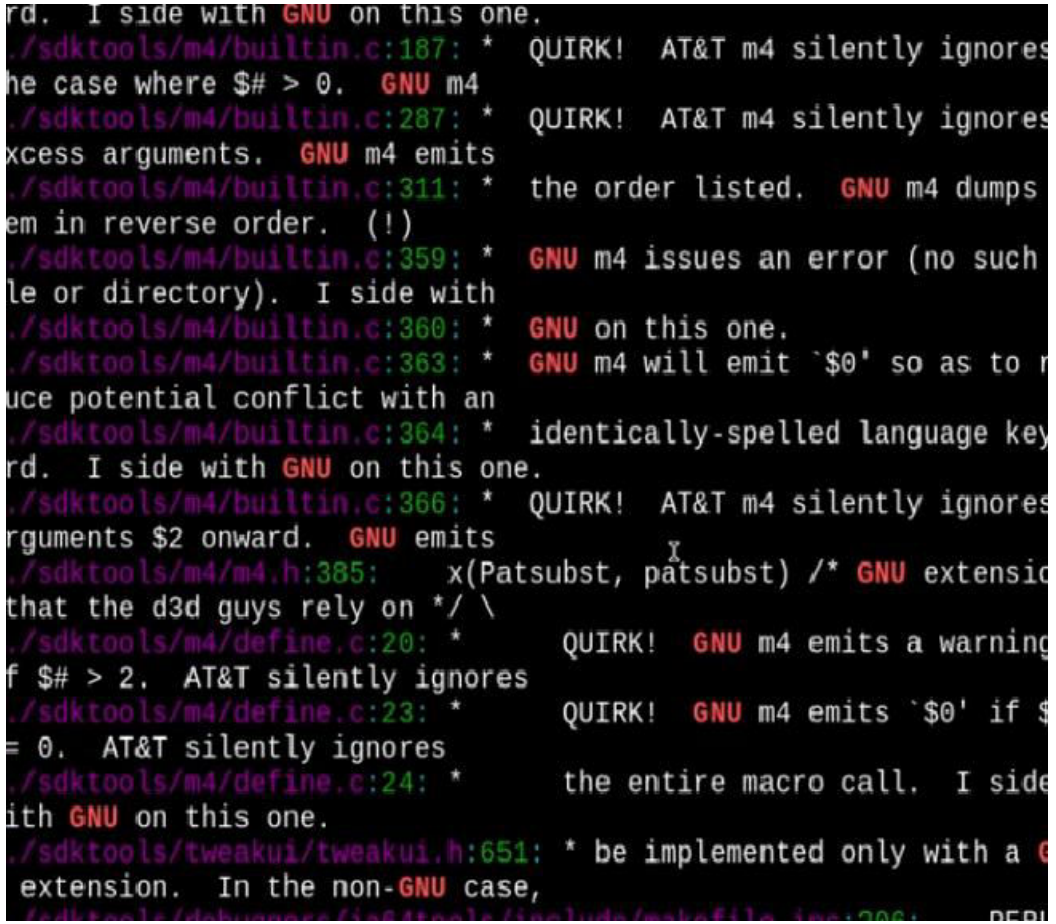
There are old 2013 patched isos which have slipstreamed sata drivers. Yes, xp was released before sata mainstream adoption.

| Name | Size |
|---|---|
| xbox | 5.29 GB |
| windows_source_bg.svg | 55.0 kB |
| windows_source_bg.png | 134 kB |
| windows_nt_4_source_code.7z | 106 MB |
| windows_nt_3_5_source_code.7z | 101 MB |
| windows_embedded_compact_2013_2015M09.7z | 93.1 MB |
| windows_embedded_ce_6_r3_170331.7z | 8.10 MB |
| windows_embedded_7_2014M12.7z | 12.8 MB |
| windows_ce_5_121231.7z | 4.91 MB |
| windows_ce_4_2_081231.7z | 3.43 MB |
| windows_ce_3_platform_builder_source_code.7z | 638 kB |
| windows_2000_source_code.7z | 122 MB |
| windows_10_shared_source_kit.7z | 74.7 MB |
| torrent description.txt | 6.62 kB |
| script | 10.3 kB |
| pdf | 31.4 MB |
| nt5src.7z | 2.36 GB |
| ms_dos_6_0_source_code.7z | 10.6 MB |
| ms_dos_3_30_oem_adaptation_kit_source_code.7z | 591 kB |
| misc | 31.1 GB |
| windows_xp_source.rar.txt | 503 B |
| windows_xp_source.rar | 367 MB |
| windows_research_kernel | 99.9 MB |
| windows ce serials.txt | 278 B |
| Windows 2000 Native API (source code).7z | 52.5 kB |
| wikileaks | 37.5 MB |
| OpenNT_final_build.7z | 1.60 GB |
| ms_patents.7z | 27.5 GB |
| misc_microsoft_gamedev_source_code.7z | 12.6 MB |
| microsoft-gaming-zone-d6f8312.7z | 3.00 MB |
| Microsoft Static Activation Key.txt | 7.55 kB |

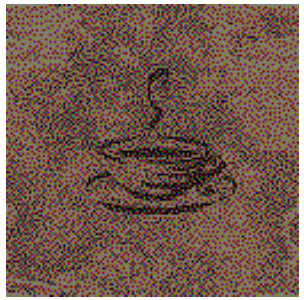


# Η Microsoft διαλέγει open source; (grep –RHIni "...")



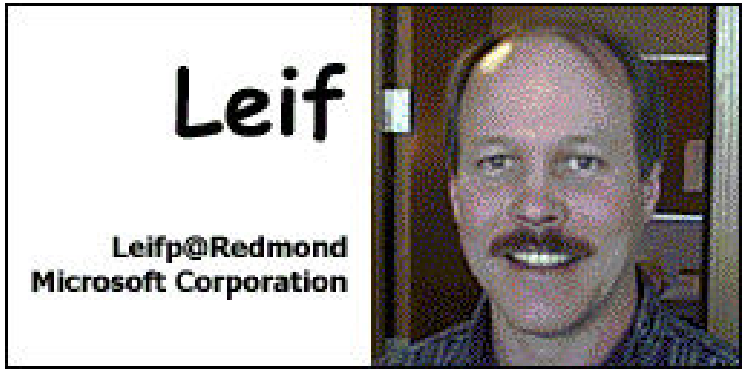
# Έχει καλλιτέχνες η Microsoft; (shell/osshell/control/bitmaps/)

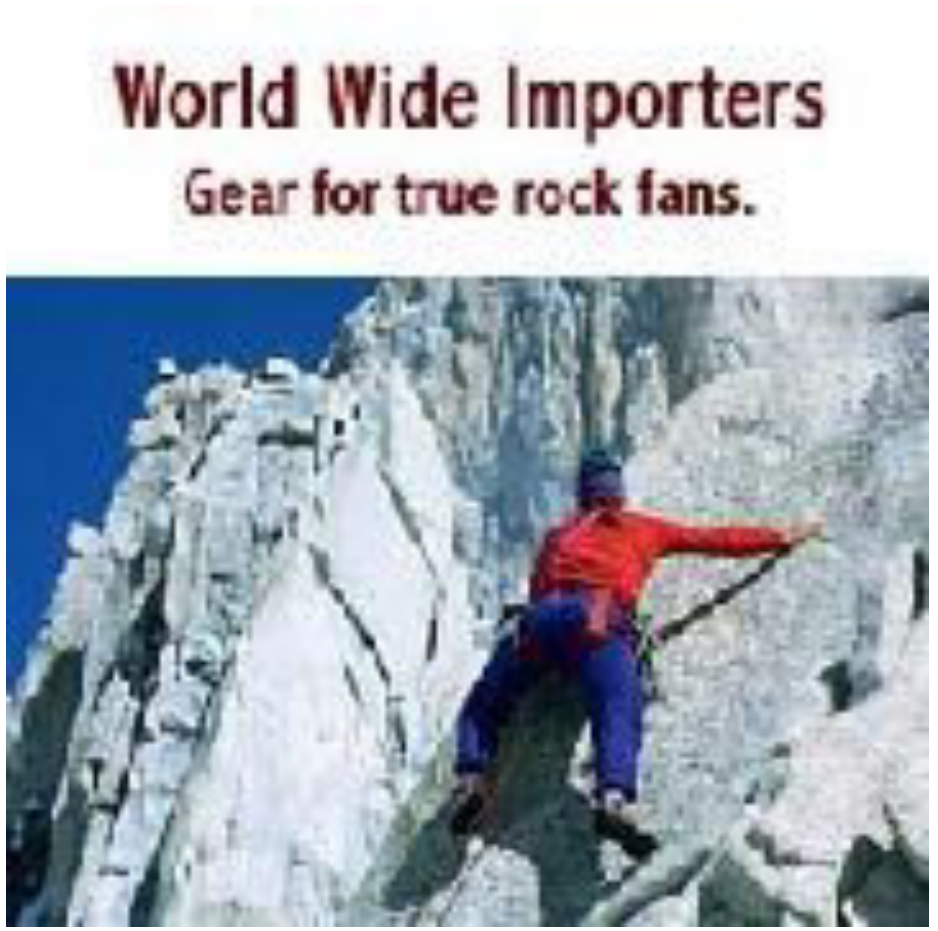
# Πού να χρησίμευε αυτό; (admin\wmi\wbem\xmltransport\samples\hairdryer)


Λίγα καρτουν ποτέ δεν έβλαψαν κανέναν (inetcore\outlookexpress\statnery.ext\deleted\cartoon char)

# Ενδιαφέρον υπάλληλοι...; (multimedia\opengl\test\misc\uidemo)

# Bill τί έκανες αυτή τη φορά; (NT\inetsrv\iis\img\help\iisnts\htm\tutorial)

# Δε θα ήταν πρόγραμμα χωρίς comments

```
//
//  Priority 5:  Hell, I don't know.  Just find some cards to pass.
//

for( i = 0 ; ( i < 4 ) && ( cPassed < 3 ) ; i++ )
```

```
// !!! We've been told not to draw, but I'm going to draw anyway, to fix bug
// WIN95C 14453.  MCIAVI draws from a keyframe forward, saying DONTDRAW on
// every frame but the last.  Works fine in theory, but in theory, communism
// works! Because of other bugs declared WONTFIX, Drawdib doesn't buffer the
// images as it goes along, so when it comes time to draw the result at the
// end, it goes "ACK! I have no idea what I was told to draw!".  So the only
// safe way to fix it is to draw even though we were told not to.  I feel safe
// doing this because this is the way VFW1.1 worked, and nobody has complained
// in over a year.
```

```
/*****************************************************************************\
    FILE: resource.rc

    DESCRIPTION:
        resource file (I can't believe I just wrote that)

    BryanSt 4/4/2000 (Bryan Starbuck)
    Copyright (C) Microsoft Corp 2000-2000. All rights reserved.
\*****************************************************************************/

#include "winres.h"
#include "resource.h"
#include "resource.rcv"



//---------------------------------------------------------------------------
//  Strings
//---------------------------------------------------------------------------
/*
STRINGTABLE DISCARDABLE
BEGIN
//    IDS_APPEARANCE_THEME_NAME                     "Windows Classic"
END
*/


// Errors
STRINGTABLE DISCARDABLE
BEGIN
    IDS_ERROR_MESSAGENUMBER                         "What are you doing, crack smoker?  %s"
    IDS_ERROR_CONVERTIMAGEFAILED                    "Converting the image failed"
END


shell/tools/starbuck/resource.rc [RO]                                         31,79
```

# Ώστε εδώ βρισκόντουσαν (shell\osshell\accesory)

| | | | |
|---|---|---|---|
| mkuni | 11/19/2020 7:38 PM | File folder | |
| testtext | 11/19/2020 7:38 PM | File folder | |
| makefile | 9/2/2002 7:24 PM | File | 1 KB |
| notepad | 9/2/2002 7:24 PM | C source file | 72 KB |
| notepad.def | 9/2/2002 7:24 PM | Export Definition ... | 1 KB |
| notepad.dlg | 9/2/2002 7:24 PM | DLG File | 4 KB |
| notepad | 9/2/2002 7:24 PM | Header file | 12 KB |
| notepad | 9/2/2002 7:24 PM | Icon | 25 KB |
| notepad.rc | 9/2/2002 7:24 PM | Resource Script | 9 KB |
| notepad.rcv | 9/2/2002 7:24 PM | RCV File | 1 KB |
| npapp | 9/2/2002 7:24 PM | Icon | 2 KB |
| npdate | 9/2/2002 7:24 PM | C source file | 2 KB |
| npfile | 9/2/2002 7:24 PM | C source file | 30 KB |
| npinit | 9/2/2002 7:24 PM | C source file | 37 KB |
| npmisc | 9/2/2002 7:24 PM | C source file | 11 KB |
| npprint | 9/2/2002 7:24 PM | C source file | 37 KB |
| nputf | 9/2/2002 7:24 PM | C source file | 4 KB |
| precomp | 9/2/2002 7:24 PM | Header file | 1 KB |
| sources | 9/2/2002 7:24 PM | File | 1 KB |
| windowsshell.manifest | 9/2/2002 7:24 PM | MANIFEST File | 1 KB |

| | | |
|---|---|---|
| access | 11/19/2020 7:37 PM | File folder |
| calc | 11/19/2020 7:37 PM | File folder |
| calendar | 11/19/2020 7:37 PM | File folder |
| clipbook | 11/19/2020 7:37 PM | File folder |
| clipbrd | 11/19/2020 7:37 PM | File folder |
| clock | 11/19/2020 7:37 PM | File folder |
| common | 11/19/2020 7:37 PM | File folder |
| eudcedit | 11/19/2020 7:37 PM | File folder |
| hypertrm | 11/19/2020 7:37 PM | File folder |
| mspaint | 11/19/2020 7:37 PM | File folder |
| netclip | 11/19/2020 7:37 PM | File folder |
| newpad | 11/19/2020 7:38 PM | File folder |
| notepad | 11/19/2020 7:38 PM | File folder |
| packager | 11/19/2020 7:38 PM | File folder |
| pbrush | 11/19/2020 7:38 PM | File folder |
| quickres | 11/19/2020 7:38 PM | File folder |
| ratpak | 11/19/2020 7:38 PM | File folder |
| spechars | 11/19/2020 7:38 PM | File folder |
| sublocal | 11/19/2020 7:38 PM | File folder |
| terminal | 11/19/2020 7:38 PM | File folder |
| uce | 11/19/2020 7:38 PM | File folder |
| ucharma2 | 11/19/2020 7:38 PM | File folder |
| ucharmap | 11/19/2020 7:38 PM | File folder |
| winchat | 11/19/2020 7:38 PM | File folder |
| wordpad | 11/19/2020 7:38 PM | File folder |

# Τζακποτ για τους χακερς (windows/winstate/doc/email/rup bug triage.xls)

| | | | |
|---|---|---|---|
| 14 | | **Trivial** | 16 |
| 15 | 234113 | C: Copying current users profile fails. The copy option should not be an available choice for current profile. | |
| 16 | 400324 | Temp profile issued to a roaming user is copied back to profile server in certain conditions | |
| 17 | 421063 | Userenv error message shows incorrect path for the users roaming profile directory. | |
| 18 | 423627 | Registry leak tracking creates too much debug output | |
| 19 | 426735 | Profile leak tracking tool AV'd on checked builds and also spews too much | |
| 20 | 429691 | LoadUserProfile should expand environment variables in members of lpProfileInfo input parameter | |
| 21 | 434826 | Post Win2K: SETUP: Setup hangs if %systemdrive%\Documents and Settings directory is encrypted. | |
| 22 | 438533 | UserProfile:ACL:Unresolved SIDs found in User Profile folder/sub-folders | |
| 23 | 439051 | Profile date displayed incorrectly due to missing conversion to local time | |
| 24 | 353345 | windows\gina\userenv\migrate.c:MigrateNT4ToNT5: stack buffer overflow (class=3.a) | |
| 25 | 354934 | *GINA: GetProfilesDirectoryEx should check return value of ExpandEnvironmentStrings | |
| 26 | 357225 | *DeleteProfile API is not setting the last error correctly in some failure cases | |
| 27 | 357240 | UnloadUserProfile causes exception when hToken parameter contains invalid (but not NULL) handle | |
| 28 | 359633 | Roaming profile pointing to a share without the \\ | |
| 29 | 379738 | Profile Applet: a user with mandatory profile can change his profile type | |
| 30 | 369711 | windows\gina\userenv\util.c:MigrateNT4ToNT5: stack buffer overflow | |

| | A | B | C | D |
|---|---|---|---|---|
| 52 | | **Bugs** | 19 | |
| 53 | 268639 | Cleanup Docs & Settings on fresh install | | |
| 54 | 341557 | All input string parameters for profile APIs should be const pointers | | |
| 55 | 452360 | Group Policy Editor: explain tab is highlighted by default | | |
| 56 | 247244 | RUP: data loss when server connection re-established | Investigate | |
| 57 | 286564 | JDP: ITG: Profile: a roaming user logon over slow link should not get error messages and temp profile when the profile server is not available | Fixed? | |
| 58 | 358788 | SetFileTime on a NetWare file is is failing with ERROR_INVALID_HANDLE | | |
| 59 | 360230 | windows\gina: many places: InitializeCriticalSection() may throw the STATUS_NO_MEMORY exception, which is not handled | | |
| 60 | 363795 | Profile Applet: "Copy To" dialog doesn't repaint itself while showing copy error message | | |
| 61 | 371743 | RC3SS: GINA\USERENV: LoadUserProfile creates named mutex with null dacl C2: | | |
| 62 | 379613 | Changing existing profile from mandatory to non mandatory does NOT work correctly | | |
| 63 | 286699 | Roaming Profiles, File Merging: Fails to recognize a renamed file | Investigate | |
| 64 | 301427 | RUP: Attributes, ACLs, compression changes to an existing file won't be propagated to the profile server if there is no file contents change ... | Investigate | |
| 65 | 346683 | RUP: Removing profile path of mandatory profile: | Investigate | |
| 66 | 372002 | RUP: Encryption warning messages remain after attribute is changed | Investigate | |
| 67 | 381085 | Profile applet: when "Copy to" destination exists, "change permission" does not apply to the existing destination when it is asked to ... | Investigate | |
| 68 | 401632 | Can't change from Mandatory profiles to roaming profiles (problem on both regular roaming profile or the TS roaming profile) | Investigate | |

# Γιατί είναι σημαντικό;

- Η πιό πρόσφατη ολοκληρωμένη ματιά μας στο πλήρη κώδικα της microsoft
- Μπορούν open-source projects όπως το Wine και το ReactOS να εμπνευστούν από των κώδικα
- Οι χακερς θα μελετήσουν το κώδικα και θα βρουν κενά ασφάλειας
- Να ξαναδωθεί μία νέα ζωή στα Windows XP

# Γιατί δεν είναι σημαντικό;

- Αν και είναι μιά ματιά στη microsoft, όχι μόνο είναι παλία αλλά ούτε η τελευταία εκδοχή των XP
- Αν υπάρχει έστω και η υποψία ότι τα λογισμικά αυτά έχουν κώδικα από τα XP τότε κινδυνεύουν
- Καθώς είναι η πιό παλιά εκδοχή τους μπορεί να υπάρχουν λιγότερα bugs
- Όλα αυτά τα forks θα είναι κρυφά και για πολύ λίγο κόσμο

# Η ρεαλιστική άποψη

- Αν και παλιά έχει ακόμη αξία
- Οι devs open-source windows προγραμμάτων θα τα αποφύγουν
- Όταν επιτίθεσαι αρκεί να βρεις ένα μόνο κενό ασφαλείας
- Είναι κωμικά γνωστό ότι πολλοί σημαντικοί τομείς σε διάφορες χώρες (κυβερνήσεις, νοσοκομεία, …) τρέχουν ακόμη XP
- Το Windows XP έχει 0.71% market share παγκοσμίως και 3.04% στην Ελλάδα (σύμφωνα με gs.statcounter)

# Μήπως το έκανε η Microsoft?

- Αυτή η θεωρία προτάθηκε από το youtube κανάλι Mental Outlaw που ειδικεύεται σε θέματα Linux. Υποστηρίζει ότι:
- Το windows XP δεν υποστηρίζεται από τη microsoft από το 2014
- Όπως είπαμε, πολλοί υπολογιστές τρέχουν windows λόγω παλιών προγραμμάτων
- Οι χακερς θα μάθουν τα προβλήματα του windows XP

# Μήπως το έκανε η Microsoft;

- Δεδομένου των προηγουμένων:
- Οι επιχειρήσεις, φοβούμενες από νέες επιθέσεις, θα προσπαθήσουν να αντιμετωπίσουν το πρόβλημα
- Κατά συνέπεια θα καταφύγουν στα Windows 10
- Έτσι θα αυξηθούν τα έσοδα και το μερίδιο της αγοράς της microsoft και ο έλεγχος του Bill πάνω μας

# Μήπως το έκανε η Microsoft

- Επίσης, θα μπορούν να πάνε ενάντιας μικρών open source προγραμμάτων (ReactOS, Wine) που επιτρέπουν non-native windows support
- Αυτά τα προγράμματα μπορούν και υπάρχουν γιατί δεν αντέγραψαν κώδικα της microsoft
- Τώρα η Microsoft χρειάζεται μόνο μία αβάσιμη υποψία για να πάει τους developers στα δικαστήρια
- Και με τη δημιουργία του Windows Subsystem for Linux, θέλουν έτσι να κλέψουν ένα market share των Linux

# Γιατί αυτό δεν ισχύει

- Οι υποστηριζόμενες εκδοχές των Windows έχουν πάνω από 90% του marketshare
- Η πιθανότητα ύπαρξης ενός σοβαρού exploit που μεταφέρεται και σε επόμενα windows είναι πιό σημαντική
- Αν πιστέψουμε τον original poster τότε όλο αυτό είναι ανεξάρτητο της microsoft
- Μέχρι και σήμερα δεν έχει ανακοινωθεί κάτι από τη microsoft, μόνο ότι κατεβάζουν torrents και repos που βρίσκουν

# Συμπερασματικά

- Το leak αν και σημαντικό δε μπορεί να έχει μεγάλο αντίκτυπο γιατί είναι copyrighted material
- Θα υπάρξουν ανανεωμένα free open-source forks του xp, αλλά θα είναι κρυφά
- Το Reactos και το wine θα πρέπει να είναι πιό προσεκτικά ως προς τους developers και τους contributors τους και δε θα το αγγίξουν
- Γενικά δεν θα επηρρεάσει πολύ την open-source κοινότητα
- Υπάρχουν καλές πιθανότητες να βγει κάποιο exploit για το xp, με εξαιρετικά μικρότερες πιθανότητες να επηρρεάζει νεότερα windows

ΑΥΤΑΑΑΑΑΑΑΑΑΑ. Ερωτήσεις;