

[Full-disclosure] – IRISH VIRUS – DoS Security Bypass and System access

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2006-03/msg01108.html>

- *From:* "Loldongs Inc" <loldongsinc@xxxxxxxxxxxx>
 - *Date:* Thu, 16 Mar 2006 21:33:29 +0000
-

=====

LOLDONGS Research 13/03/2006

– Internet 1.0 DoS Security Bypass and System access – IRISH VIRUS –

Table of Contents

Affected Software.....	1
Severity.....	2
Description of Vulnerability.....	3
Proof of Concept.....	4
Solution.....	5
Time Table.....	6
Credits.....	7
References.....	8
About LOLDONGS Inc.....	9
Verification.....	10

1) Affected Software

a) List of affected operating systems

- * CTSS (The Compatible Timeshare System)
- * Incompatible Timesharing System (ITS, developed at MIT)
- * THE operating system (by Dijkstra et al.)
- * Multics (joint OS development project by Bell Labs, GE, and MIT)
- * Master programme (developed for Leo Computers, Leo III in 1962)
- * RC 4000 Multiprogramming System (
- * Apple Computer Apple DOS
- * Business Operating System (BOS)
- * Commodore PET, Commodore 64, and Commodore VIC-20,
- * The very first IBM-PC
- * Sinclair Micro and QX, etc
- * TRS-DOS, ROM OS's (largely Microsoft BASIC implementations)
- * TI99/4A

- * Flex
- * FLEX9 (by TSC for Motorola 6809 based micros)
- * mini-FLEX (by TSC for 5.25" disks on 6800 based machines)
- * CMT-ROS
- * Arthur
- * ARX
- * BBC OS
- * RISC OS
- * RISC iX
- * AmigaOS
- * AMIX (Amiga Unix SVR4)
- * Apple DOS
- * ProDOS
- * GS/OS
- * Lisa OS
- * A/UX
- * Mac OS
 - o System 6
 - o System 7 (code-named "Big Bang")
 - o Mac OS 8
 - o Mac OS 9
 - * Mac OS X
 - o Mac OS X v10.0 (aka Mac OS X 10.0 "Cheetah")
 - o Mac OS X v10.1 (aka Mac OS X 10.1 "Puma")
 - o Mac OS X v10.2 (aka Mac OS X 10.2 "Jaguar")
 - o Mac OS X v10.3 (aka Mac OS X 10.3 "Panther")
 - o Mac OS X v10.4 (aka Mac OS X 10.4 "Tiger")
 - o Mac OS X v10.5 (aka Mac OS X 10.5 "Leopard")
 - * Mac OS X Server
- * Darwin (open source underpinnings to MacOS X)
- * ArrayOS
- * TOS
- * MultiTOS
- * MiNT
- * BTOS
- * MCP
- * CTOS
- * BeOS
 - o BeIA
- * ZETA (formerly BeOS)
- * AIS
- * OS/8
- * ITS (for the PDP-6 and PDP-10)
- * MPE (from HP)
- * TOPS-10 (for the PDP-10)
- * WAITS
- * TENEX (from BBN)
- * TOPS-20 (for the PDP-10)
- * RSTS/E (ran on several machines, chiefly PDP-11s)
- * RSX-11 (multiuser, multitasking OS for PDP-11s)
- * RT-11 (single user OS for PDP-11)

[Full-disclosure] – IRISH VIRUS – DoS Security Bypass and System access

- * VMS (by DEC for the VAX mini-computer range)
- * Domain/OS (originally Aegis, from Apollo Computers)
- * HP-UX
- * Ultrix
- * Digital UNIX (derived from OSF/1, and which became HP's Tru64)
- * NonStop Kernel Supports concurrent execution of:
 - o Guardian
 - o OSS (POSIX-compliant Open System Services)
- * PC-DOS
- * OS/2 (developed jointly with Microsoft)
 - o OS/2 Warp
 - o eComStation (licensed to Serenity Systems International)
- * Basic Operating System
- * TOS
- * OS/360 (first OS planned for the System 360 architecture)
- * DOS/360
- * DOS/VSE
- * z/VSE (latest version of the VSE line)
- * VM/CMS
- * z/VM (latest version of the VM line)
- * MFT (later called OS/VS1)
- * MVT (later called OS/VS2)
- * SVS
- * MVS (latest variant of MVT)
- * TPF
- * OS/390
- * z/OS, Unix-like, (latest version of IBM mainframe OS)
- * i5/OS formerly OS/400
- * AIX (a version of Unix)
- * AOS (a version of BSD Unix)
- * ALCS
- * IBSYS
- * DPPX
- * K42
- * Xenix (licensed version of Unix; sold to SCO in '90s)
- * MS-DOS (developed jointly with IBM, versions 1.0?6.22)
- * Windows CE (OS for handhelds and embedded devices)
 - o Windows CE 3.0
 - o Windows Mobile (based on Windows CE)
 - o Windows CE 5.0
- * Microsoft Windows
 - o Windows 1.0
 - o Windows 2.0
 - o Windows 3.0
 - o Windows 3.1x
 - o Windows 3.2 (Chinese only release)
 - o Windows 95 (aka Windows 4.0)
 - o Windows 98 (aka Windows 4.1)
 - o Windows Me (aka Windows 4.2)
- * OS/2 (developed jointly with IBM)
- * Windows NT

- o Windows NT 3.1
- o Windows NT 3.5
- o Windows NT 3.51
- o Windows NT 4.0
- o Windows 2000 (aka Windows NT 5.0)
- o Windows XP (aka Windows NT 5.1)
- o Windows Server 2003 (aka Windows NT 5.2)
- o Windows Vista (to be released in July 2006)
- o Windows Longhorn Server
- * Desqview
- * EOS (Operating System)
- * GCOS (originally developed by General Electric)
- * NCR IRX (operating system used by NCR I-9040 series)
- * THEOS (THEOS Software Corporation)
- * TinyOS
- * TX/4 and DX/10 (for TI 990 minicomputers)
- * Aegis (Apollo Computers)
- * AMIX (Amiga porting of Unix System V release 3.1)
- * Cromix (Unix-like OS from Cromemco)
- * Coherent (Unix-like OS)
- * DNIX
- * Idris workalike from Whitesmiths
- * IRIX from SGI
- * Mac OS X from Apple Computer
- * NeXTSTEP (developed by NeXT)
- * OS-9 Unix-like RTOS. (for Motorola 6809 based microcomputers)
- o OS-9/68k (for Motorola 680x0 based computers)
- o OS-9000 (portable Unix emulating OS from Microware)
- * OSF/1 (by Digital Equipment Corporation)
- * OPENSTEP
- * QNX (POSIX, microkernel OS; usually a real time embedded OS)
- * Rhapsody
- * RISC/os (a port by MIPS of 4.3BSD to the MIPS RISC architecture)
- * RMX
- * SCO UNIX (from SCO, bought by Caldera)
- * SINIX (a port by SNI of Unix to the MIPS RISC architecture)
- * Solaris (Sun's System V-based replacement for SunOS)
- * SunOS (BSD-based Unix system used on early Sun hardware)
- * System V (a release of AT&T Unix, 'SVr4' was the 4th minor release)
- * UniFlex (Unix emulating OS by TSC for Motorola 6809 based)
- * UniCOS
- * MUSIC/SP (for the S/370, running normally under VM)
- * SkyOS (developed by Robert Szeleney)
- * EXEC I
- * EXEC II
- * EXEC 8
- * OS-1100
- * OS-1200
- * OS/3
- * Unix (OS developed at Bell Labs ca 1970)

- * Minix (study OS developed by Andrew S. Tanenbaum)
- * Amoeba (research OS by Andrew S. Tanenbaum)
- * Plan 9 (distributed OS developed at Bell Labs)
- * Inferno (distributed OS originally from Bell Labs)
- * Plan B (distributed OS derived from Plan 9)
- * Xinu, (Study OS developed by Douglas E. Comer in the USA)
- * Solaris, contains original Unix (SVR4) code
- * OpenSolaris, contains original Unix (SVR4) code
- * BSD (Berkeley Software Distribution)
 - o FreeBSD
 - o DragonFly BSD forked from FreeBSD
 - o NetBSD
 - o OpenBSD forked from NetBSD
- * Linux
- * OpenDarwin
- * GNU Hurd
- * SSS-PC Developed at Tokyo University
- * Mach (from OS kernel research at Carnegie Mellon University)
- * Nemesis
- * TUNES, 1994
- * V (operating system) from Stanford, early 1980s
- * L4 Second generation microkernel
- * ILIOS (Research OS designed for routing purposes.)
- * ReactOS (A free software Windows NT compatible OS)
- * FreeDOS (an open source DOS variant)
- * QDOS (also called SCP-DOS; became MS-DOS/PC-DOS)
 - o MS-DOS
 - o PC-DOS (IBM's DOS variant)
- * DR-DOS (Digital Research's DOS variant)
 - o Concurrent DOS (first Multiuser variant of DOS)
 - o Multiuser DOS (later Multiuser variant of DOS)
- * FreeDOS (an open source DOS variant)
- * Inferno
- * Cambridge Ring O/S
- * CSIRONET (CSIRO)
- * NegrOS
- * CTOS (Convergent Technologies, later acquired by Unisys)
- * NOS (for use in CDC's Cyber line of supercomputers)
- * Brocade Fabric OS
- * BLIS/COBOL
- * Bluebottle (AOS)
- * BS1000 (Siemens AG)
- * BS2000 (Siemens AG, now BS2000/OSD)
- * BS3000 by Siemens AG (similar to OS-IV and MSP from Fujitsu)
- * Control Program/Monitor (CP/M)
 - o CP/M-80 (CP/M for Intel 8080/8085 and Zilog Z80)
 - o CP/M-86 (CP/M for Intel 8088/86 from Digital Research)
 - o MP/M-80 (Multi programming version of CP/M-80)
 - o MP/M-86 (Multi programming version of CP/M-86)
- * DESQview (multi-tasking windowing user interface for DOS)
 - o DESQView/X (X-windowing GUI for DOS)

[Full-disclosure] – IRISH VIRUS – DoS Security Bypass and System access

- * FLEX9 (by TSC for Motorola 6809 based machines)
- * GEM (windowing GUI for CP/M, DOS, and Atari TOS)
- * GEOS (popular windowing GUI for PC, Commodore, Apple computers)
- * JavaOS
- * Jnode (JNode.org's OS written 99% in Java (native compiled))
- * KERNAL (default OS on Commodore 64)
- * MorphOS (by Genesi)
- * MSP by Fujitsu (successor to OS-IV), now MSP/EX for 31-bit mode
- * nSystem by Luis Mateu at DCC, Universidad de Chile
- * NetWare (networking OS by Novell)
- * Oberon operating system
- * OSD/XC (by Fujitsu-Siemens)
- * OS-IV by Fujitsu (based on early versions of IBM's MVS)
- * Pick (often licensed and renamed)
- * LOLBBQOS
- * PRIMOS by Prime Computer (sometimes spelled PRIMOS and PRIME)
- * SEAL System is a free 32-bit GUI for DOS.
- * SkyOS (Commercial desktop OS for PCs)
- * SSB-DOS (by TSC for Smoke Signal Broadcasting)
- * TripOS, 1978
- * JEWSDIDWTC Operative System (By Luldongs Inc.)
- * UCSD p-System
- * VME by International Computers Limited (ICL)
- * VOS by Stratus Technologies with strong influence from Multics
- * VOS by Hitachi for its IBM-compatible mainframes
- * VM2000 by Siemens AG
- * VisiOn (first GUI for early PC machines)
- * aceos under GPL
- * ANDOS
- * MK-DOS
- * CSI-DOS
- * NORD
- * ?? ??-11 (a version of RT-11)
- * AO-DOS
- * BASIS
- * DOSB10
- * PascalDOS
- * MicroDOS
- * DX-DOS
- * HC-DOS
- * RT-11 (ROM embedded)
- * NORTON-??
- * ?????
- * KMON
- * Turbo-DOS
- * Agnix
- * AMOS
- * AROS (Amiga Research Operating System)
- * AtheOS became Syllable
- * BlueIllusion OS
- * BOS – 100% assembler OS

- * Brainix
- * CalotaOS (Calota Software Labs Operating System)
- * Clicker
- * Desert Spring-Time – An Ocaml based operating system
- * EROS
- * Glider
- * Haiku (open source BeOS clone)
- * HelenOS
- * IsaacOS
- * LainOS
- * LSE/OS
- * MenuetOS (compact OS written entirely in FASM assembly language)
- * MMURTL (written by Richard Burgess; presented in MMURTL V1.0)
- * NewOS
- * Panalix
- * Sanos (Minimalistic x86 OS kernel)
- * SOFregit (Operating System for educational purposes)
- * Syllable (a modern, independently originated OS; see AtheOS)
- * Tabos (a rescue/network/desktop system)
- * Trion Operating System
- * Unununium
- * Visopsys
- * ROM-DOS
- * Embedded Linux
- * Minix version 3
- * Windows Embedded
- * Palm OS from Palm Inc; now spun off as PalmSource
- * EPOC (originally from Psion (UK), now from Symbian)
- * Windows CE Windows Compact Edition, from Microsoft
 - o Pocket PC from Microsoft, a variant of Windows CE.
 - o Windows Mobile from Microsoft, a variant of Windows CE.
- * Linux on Sharp Zaurus and Ipaq
- * DOS on Poqet PC
- * Newton OS on Apple Newton Messagepad
- * Windows CE
- * Embedded Linux, MontaVista Linux in Motorola's A760, E680
- * Mobilinux by Montavista.
- * Symbian OS
- * Cisco IOS (originally Internetwork Operating System)
- * IOS-XR by Cisco Systems
- * CatOS by Cisco Systems
- * PIX OS by Cisco Systems
- * JUNOS by Juniper Networks
- * ROS by Ruggedcom
- * Contiki written in C programming language
- * LUnix written in 6502
- * eCos
- * FreeRTOS
- * INTEGRITY
- * LynxOS
- * OSEK

- * MontaVista Linux
- * Nucleus
- * OS-9 by Microware
- * QNX
- * Rtems
- * RTLinux
- * Salvo
- * ThreadX
- * TRON (also ITRON, BTRON, CTRON, MTRON, etc.)
- * μ CLinux
- * VRTX
- * VxWorks
- * XMK (eXtreme Minimal Kernel)
- * Operating System Embedded usually known as OSE
- * Par-OS
- * J98
- * GWOS
- * Swodniw
- * Finux
- * ALTIMIT OS
- * Hyper OS
- * Wheatonix
- * Digitronix
- * Luna/X
- * Copland OS
- * LCARS
- * NNIX
- * Jesus
- * lesbian GNU/Linux
- * HelicacOS
- * BrickOS operating system
- * leJOS operating system

b) List of affected email clients

- * acme Mail – interface for upas
- * Aethera
- * Apple Mail
- * Balsa
- * Becky!
- * Bloomba
- * Citadel
- * Claris Em@iler
- * Eudora
- * Forté Agent
- * GroupWise
- * IncrediMail
- * KMail
- * Lotus Notes
- * Opera M2

- * Microsoft Entourage
- * Microsoft Outlook
- * Microsoft Outlook Express
- * Mozilla Thunderbird
- * Mozilla Mail & Newsgroups
- * Mulberry
- * Netscape
- * Novell Evolution
- * Pegasus Mail
- * i.Scribe/InScribe
- * SeaMonkey Mail & Newsgroups
- * Sylpheed
- * The Bat!
- * YAM (Yet Another Mailer)
- * Elm
- * Elmo
- * Gnus
- * mailx(1) ? one of the traditional mail(1) implementations
- * MH
- * Mutt
- * Pine
- * Upas ? e-mail filesystem (from Plan9)
- * Citadel
- * Horde IMP
- * Hula project
- * WebPine
- * RoundCube Webmail
- * Skweezer Mail
- * SquirrelMail
- * Zimbra
- * Calypso
- * Netscape Communicator

Other versions may also be affected.

2) Severity

Rating: ULTRA MEGA Extremely Critical

Impact: DoS (Denial of Service), Security Bypass and System access

Where: Remote and Local

3) Description of Vulnerability

LOLDONGS Research, a Wholly Owned Subsidiary of Banned Town Security Inc., has discovered a vulnerability in Internet 1.0, which can be exploited by clever people to rape morons in the ass.

This vulnerability affects EVERY SINGLE computarmachine capable of displaying text and/or images.

EVERY OPERATIVE SYSTEM, EMAIL CLIENT, COMPUTARMACHINE, CELL PHONE AND TELETYPE TERMINAL IS AFFECTED.

The vulnerability is caused due to a stupidity overflow error in the brain of a clearly retarded user; causing the user to malfunction, therefore bypassing security and carrying out a Denial of Service in the remote machine. A more advanced attack may also give a malicious user(read: someone who's not a total fucktard) BOFH-LOLZ-JIZZTAPO priviledges.

4) Proof of Concept

a) By any means, display the following sequence of characters in a computarmachine display interface:

Greetings, You have just received the "IRISH VIRUS". As we don't have any programming experience, this Virus works on the honour system. Please delete all the files on your hard drive manually and forward this Virus to everyone on your mailing list. Thank you for your cooperation.

b) By any means, display the following image in a graphics enabled computarmachine:

<http://tinypic.com/rbwg14.jpg>

5) Solution

There are no known solutions or workarounds.

6) Time Table

20/08/2002 – Initial vendor notification.
24/09/2002 – Initial vendor reply.
??/??/???? – PROFIT!
13/03/2006 – Public disclosure.

7) Credits

Discovered by Jimmy the Jew Gasser, Banned Town Security Inc.

8) References

The Common Vulnerabilities and Exposures (CVE) project has assigned CVE-0500BC-0001 for the vulnerability.

9) About LOLDONGS Inc.

LOLDONGS collects, validates, assesses and writes advisories which make fun of stupid Whitehat-wannabees and Script-Kiddies who hang out at the Full-Disclosure Mailing List. These advisories are gathered in a publicly available database at the LOLDONGS website:

<http://advisories.on.nimp.org/>

LOLDONGS offers services to our customers enabling them to receive all relevant BBQ-jizz-poopoo information to their specific rectum configuration.

LOLDONGS offers FREE buttseckz guides called "LOLDONGS In Ur Ass":

http://advisories.on.nimp.org/loldongs_security_advisories/

10) Verification

Please verify this advisory by visiting the LOLDONGS Inc website:

http://advisories.on.nimp.org/loldongs_research/0500BC-0001/advisory/

Complete list of vulnerability reports published by LOLDONGS Research:

http://advisories.on.nimp.org/loldongs_research/

Don?t just search. Find. Check out the new MSN Search!

<http://search.msn.click-url.com/go/onm00200636ave/direct/01/>

Full-Disclosure – We believe in it.

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

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