project-zero project-zero New issue All issues Search project-zero issues... Sign in

1 - 100 of 1866 Next › List Grid Chart

ID	Status	Restrict	Reported	Vendor	Product	Finder	Summary + Labels
1	Invalid	----	----	Test	----	----	This is a test
9	Fixed	----	----	Apple	Safari	ianbeer	Safari sandbox logic error enables reading of arbitrary files
10	Fixed	----	2014-Apr-04	Apple	Safari	ianbeer	Safari sandbox IPC memory corruption with WebEvent::Wheel
11	Fixed	----	2014-Apr-04	Apple	Safari	ianbeer	Safari sandbox IPC memory corruption with WebEvent::Char
12	Fixed	----	2014-Apr-04	Apple	OSX	ianbeer	launchd heap corruption due to integer overflow in launch_data_unpack
13	Fixed	----	2014-Apr-04	Apple	OSX	ianbeer	launchd heap corruption due to incorrect rounding in launch_data_unpack
14	Fixed	----	2014-Apr-04	Apple	OSX	ianbeer	launchd heap overflow in log_forward
15	Fixed	----	2014-Apr-04	Apple	iOS, OSX	ianbeer	Lack of bounds checking in notifyd CCProjectZeroMembers
16	Fixed	----	2014-Apr-04	Apple	OSX	ianbeer	launchd heap corruption due to unchecked strcpy in init_session MIG ipc
17	Fixed	----	2014-May-02	Apple	OSX-Kernel	ianbeer	OS X IOKit kernel code execution due to lack of bounds checking in IOAccel2DContext2::blit
18	Fixed	----	2014-May-02	Apple	OSX-Kernel	ianbeer	OS X IOKit kernel memory disclosure due to lack of bounds checking in AGPMClient::getPstatesOccupancy
19	Fixed	----	2014-May-03	Apple	OSX-Kernel	ianbeer	OS X IOKit kernel code execution due to unchecked pointer parameter in IGAccelCLContext::unmap_user_memory
20	Fixed	----	2014-May-06	Apple	OSX-Kernel	ianbeer	OS X IOKit Multiple exploitable kernel NULL dereferences (x4)
21	Fixed	----	----	Apple	OSX-Kernel	ianbeer	OS X IOKit kernel memory disclosure due to lack of bounds checking in IOUSBControllerUserClient::ReadRegister
22	Fixed	----	2014-May-20	Apple	OSX-Kernel	ianbeer	OS X IOKit kernel code execution due to incorrect bounds checking in Intel GPU driver (x2)
23	Fixed	----	2014-May-21	Apple	OSX-Kernel	ianbeer	OS X kASLR defeat using sgdt
24	Fixed	----	2014-May-22	Apple	OSX-Kernel	ianbeer	OS X IOKit kernel code execution due to NULL pointer dereference in IOThunderboltFamily
28	Fixed	----	2014-Jun-06	Apple	OSX-Kernel	ianbeer	OS X IOKit kernel code execution due to lack of bounds checking in GPU command buffers
29	Fixed	----	2014-Jun-10	Apple	OSX-Kernel	ianbeer	OS X IOKit kernel code execution due to off-by-one error in IGAccelGLContext::processSidebandToken
30	Fixed	----	2014-Jun-12	Apple	OSX-Kernel	ianbeer	OS X IOKit kernel multiple exploitable memory safety issues in token parsing in IGAccelVideoContextMedia (x5)
31	Fixed	----	2014-Jun-12	Apple	OSX-Kernel	ianbeer	OS X IOKit kernel code execution due to NULL pointer dereference in IOAccelContext2::clientMemoryForType
32	Fixed	----	2014-Jun-13	Apple	OSX-Kernel	ianbeer	OS X IOKit kernel code execution due to lack of bounds checking in IGAccelVideoContextMain::process_token_ColorSpaceConversion
33	Fixed	----	2014-Jun-16	Apple	OSX-Kernel	ianbeer	OS X IOKit kernel code execution due to lack of bounds checking in IOAccelDisplayPipeTransaction2::set_plane_gamma_table
34	Fixed	----	2014-Jun-17	Apple	OSX-Kernel	ianbeer	OS X IOKit kernel code execution due to multiple bounds checking issues in IGAccelGLContext token parsing (x3)
35	Fixed	----	2014-Jun-18	Apple	OSX-Kernel	ianbeer	OS X IOKit kernel code execution due to controlled kmem_free size in IOSharedDataQueue
36	Fixed	----	2014-Jun-20	Apple	iOS-Kernel, OSX-Kernel	ianbeer	OS X IOKit kernel code execution due to lack of bounds checking in AppleMultitouchIODataQueue
37	Fixed	----	2014-Jun-23	Apple	OSX-Kernel	ianbeer	OS X IOKit kernel code execution due to bad free in IOBluetoothFamily
38	Fixed	----	2014-Jun-23	Apple	OSX-Kernel	ianbeer	OS X IOKit kernel code execution due to integer overflow in IOBluetoothDataQueue (root only)
39	Fixed	----	2014-Jun-26	Apple	iOS-Kernel, OSX-Kernel	ianbeer	OS X IOKit kernel code execution due to integer overflow in IODataQueue::enqueue
40	Fixed	----	2014-Jun-30	Apple	iOS-Kernel, OSX-Kernel	ianbeer	OS X IOKit kernel code execution due to heap overflow in IOHIKeyboardMapper::parseKeyMapping
41	Fixed	----	2014-Jun-30	Apple	iOS-Kernel, OSX-Kernel	ianbeer	OS X IOKit kernel code execution due to NULL pointer dereference in IOHIKeyboardMapper::stickyKeysfree
42	Fixed	----	2014-Jul-07	Apple	iOS-Kernel, OSX-Kernel	ianbeer	OS X IOKit kernel memory disclosure due to lack of bounds checking in IOHIKeyboardMapper::modifierSwapFilterKey
43	Fixed	----	2014-Jul-8	Adobe	Flash	cevans	Flash leak of uninitialized data whilst rendering JPEGs
44	Fixed	----	2014-Jul-9	Adobe	Flash	cevans	Flash leak of uninitialized data whilst rendering a 2-component JPEG
45	Fixed	----	2014-Jul-14	Adobe	Flash	cevans	Flash leak of uninitialized memory when rendering valid(?) 1bpp image
46	Fixed	----	2014-Jul-14	Adobe	Flash	cevans	Flash heap buffer overflow calling copyPixelsToByteArray() on a large ByteArray CCProjectZeroMembers
47	Fixed	----	2014-Jul-14	Adobe	Flash	cevans	Flash leak of uninitialized data when image zlib stream ends prematurely CCProjectZeroMembers
48	Fixed	----	2014-Jul-14	Adobe	Flash	cevans	Flash leak of uninitialized data when JPEG image alpha channel zlib stream ends prematurely CCProjectZeroMembers
71	Fixed	----	2014-Jul-16	Adobe	Flash	cevans	Flash out-of-bounds read in uploadCompressedTextureFromByteArray() CCProjectZeroMembers
75	Fixed	----	2014-Jul-21	Adobe	Flash	cevans	Flash out-of-bounds read with empty ID3 tag CCProjectZeroMembers
76	Fixed	----	2014-Jul-23	Adobe	Flash	cevans	Flash memory corruption (double free?) with RTMP packet that aborts itself CCProjectZeroMembers
77	Duplicate	AddIssueComment-Commit	----	Apple	Safari	ianbeer	WebKit JavaScriptCore integer truncation vulnerability
78	Fixed	----	2014-Jul-25	Adobe	Flash	cevans	Flash memory corruption (integer overflow?) concatenating strings to ~4GB in size CCProjectZeroMembers
79	Fixed	----	2014-Jul-28	Adobe	Flash	cevans	Flash out-of-bounds read with large string length in RTMP packet CCProjectZeroMembers
80	Fixed	----	2014-Jul-30	Apple	OSX	ianbeer	OS X coresymbolicationd multiple user to root privilege escalations due to XPC type confusion CCProjectZeroMembers
82	Fixed	----	2014-Jul-31	Adobe	Flash	cevans	Flash out-of-bounds read in uploadCompressedTextureFromByteArray() [CubeTexture variant] CCProjectZeroMembers
84	Fixed	----	2014-Aug-7	PHP	PHP	groebert	Out-of-bounds read in php_parserr with user-supplied dlen CCProjectZeroMembers
88	Fixed	----	2014-Aug-15	Linux	Kernel	cevans	Linux kernel stack overflow when mounting ISO9660 image, including via a USB stick CCProjectZeroMembers
89	Fixed	----	2014-Aug-18	Linux	Kernel	hawkes	Linux kernel hid-logitech-dj.c device_index arbitrary kfree CCProjectZeroMembers

90	Fixed	----	2014-Aug-18	Linux	Kernel	hawkes	Linux kernel hid-logitech-dj.c logi_dj_ll_raw_request heap overflow CCProjectZeroMembers
91	Fixed	----	2014-Aug-18	Linux	Kernel	hawkes	Linux kernel HID report fixup multiple off-by-one issues CCProjectZeroMembers
92	Fixed	----	2014-Aug-18	Apple	OSX	ianbeer	OS X sandbox escape due to XPC type confusion in networkd CCProjectZeroMembers
93	Fixed	----	2014-Aug-18	Adobe	Flash	ianbeer	Flash memory corruption in Actionscript 2 Array.join CCProjectZeroMembers
94	Fixed	----	2014-Aug-19	Adobe	Reader	forshaw	Windows Acrobat Reader 11 Sandbox Escape in NtSetInformationFile CCProjectZeroMembers
95	Fixed	----	2014-Aug-20	Microsoft	IE	forshaw	IE11 ImmutableApplicationSettings EPM Privilege Escalation CCProjectZeroMembers
96	Fixed	----	2014-Jul-13	glibc	glibc	taviso	glibc off-by-one NUL byte heap overflow in gconv_translit_find CCProjectZeroMembers
97	Fixed	----	2014-Aug-21	Microsoft	IE	forshaw	IE11 EPM Parent Process DACL Sandbox Escape CCProjectZeroMembers
98	Fixed	----	2014-Aug-22	Linux	Kernel	forshaw	Linux Kernel Buffer Overflow in Whiteheat USB Serial Driver CCProjectZeroMembers
99	Fixed	----	2014-Aug-25	Microsoft	IE	forshaw	IE11 AudioSrv RegistryKey EPM Privilege Escalation CCProjectZeroMembers
100	Fixed	----	2014-Aug-25	Linux	Kernel-HID	scvitti	Magic Mouse HID device driver overflow CCProjectZeroMembers
101	Fixed	----	2014-Aug-25	Linux	Kernel	scvitti	PicoLCD HID device driver pool overflow CCProjectZeroMembers
103	Fixed	----	2014-Aug-27	Adobe	Reader	forshaw	Windows Acrobat Reader 11 Sandbox Escape in MoveFileEx IPC Hook CCProjectZeroMembers
106	Fixed	----	----	Adobe	Flash	ianbeer	Flash logic error in bytecode verifier CCProjectZeroMembers
107	Fixed	----	2014-Sep-15	Microsoft	Office-2007	hawkes	Microsoft Office 2007 TTDeleteEmbeddedFont handle double delete CCProjectZeroMembers
108	Fixed	----	2014-Sep-15	Microsoft	Office-2007	hawkes	Microsoft Office 2007 lcbPlcffndTxt/fcPlfguidUim memory corruption CCProjectZeroMembers
109	Fixed	----	----	Adobe	Flash	ianbeer	Flash heap overflow in bytecode verifier CCProjectZeroMembers
110	Fixed	----	2014-Sep-17	Microsoft	Office-2007	hawkes	Microsoft Office 2007 PapxFkp rgbx bOffset memory corruption CCProjectZeroMembers
111	Fixed	----	2014-Sep-17	Microsoft	Office-2007	hawkes	Microsoft Office 2007 VBA ExtendedControl use-after-free CCProjectZeroMembers
112	Fixed	----	----	Adobe	Flash	ianbeer	Adobe Flash incorrect jit optimization with op_pushwith CCProjectZeroMembers
113	Fixed	----	2014-Sep-22	Adobe	Flash	Fermin	Flash 14 on IE11, readAV crash on xmm instruction CCProjectZeroMembers
114	Fixed	----	----	Adobe	Flash	ianbeer	Adobe Flash incorrect jit optimization with op_pushscope CCProjectZeroMembers
115	Fixed	----	----	Adobe	Flash	ianbeer	Adobe Flash incorrect jit optimization with op_setglobalslot CCProjectZeroMembers
116	Fixed	----	2014-Sep-24	Adobe	Flash	external	Flash heap buffer overflow calling Camera.copyToByteArray() with a large ByteArray CCProjectZeroMembers
117	Fixed	----	2014-Sep-29	Microsoft	Office-2007	hawkes	Microsoft Office 2007 MsoDrawingGroup rgChildRec invalid GlobalFree CCProjectZeroMembers
118	Fixed	----	2014-Sep-30	Microsoft	Windows-Kernel	forshaw	Windows: Elevation of Privilege in ahcache.sys/NtApphelpCacheControl CCProjectZeroMembers
119	Fixed	----	2014-Sep-30	Microsoft	Office-2007	hawkes	Microsoft Office 2007 BoundSheet dt use-after-free CCProjectZeroMembers
120	Fixed	----	2014-Oct-3	Adobe	Flash	natashenka	Type Confusion in Setting Microphone Codec CCProjectZeroMembers
121	Fixed	----	2014-Oct-07	Apple	OSX	ianbeer	OS X privilege escalation due to XPC type confusion in sysmond (with exploit) CCProjectZeroMembers
122	Fixed	----	2014-Oct-7	Adobe	Flash	taviso, cevans	Flash memory corruption in the G711 codec with 4-byte samples CCProjectZeroMembers
123	Fixed	----	2014-Oct-13	Microsoft	Windows	forshaw	Windows Elevation of Privilege in User Profile Service CCProjectZeroMembers
124	Fixed	----	2014-Oct-13	Adobe	Flash	taviso, cevans	Flash memory corruption when upper casing malformed Unicode CCProjectZeroMembers
125	Fixed	----	2014-Oct-14	Adobe	Flash	taviso, cevans	Flash corruption after corrupting pre-validated bytecode CCProjectZeroMembers
126	Invalid	----	2014-Oct-14	Apple	OSX	ianbeer	OS X kASLR defeat due to kernel pointers in IOKit registry CCProjectZeroMembers
127	WontFix	----	2014-Oct-17	Microsoft	Windows-Kernel	forshaw	Windows 7: Admin Check Bypass in NtPowerInformation CCProjectZeroMembers
128	Fixed	----	2014-Oct-17	Microsoft	Windows-Kernel	forshaw	Windows: Impersonation Check Bypass With CryptProtectMemory and CRYPTPROTECTMEMORY_SAME_LOGON flag CCProjectZeroMembers
129	Fixed	----	2014-Oct-17	Microsoft	Office-2007	hawkes	Microsoft Office 2007 dispatch table out-of-bounds function call CCProjectZeroMembers
130	Fixed	----	2014-Oct-20	Apple	OSX	ianbeer	OS X networkd "effective_audit_token" XPC type confusion sandbox escape (with exploit) CCProjectZeroMembers
131	Fixed	----	2014-Oct-20	Adobe	Flash	taviso, cevans	Flash write crash at NULL + 0x2b288 (on 64-bit) CCProjectZeroMembers
132	Fixed	----	2014-Oct-20	Microsoft	Office-2007	hawkes	Microsoft Office 2007 shape drawing object use-after-free CCProjectZeroMembers
135	Fixed	----	2014-Oct-21	Apple	IOKit	ianbeer	OS X IOKit kernel code execution due to NULL pointer dereference in IntelAccelerator CCProjectZeroMembers
136	Fixed	----	2014-Oct-23	Apple	IOKit	ianbeer	OS X IOKit kernel memory corruption due to bad bzero in IOBluetoothDevice CCProjectZeroMembers
137	Fixed	----	2014-Oct-24	Microsoft	Windows-Kernel	forshaw	Windows: Impersonation Check Bypass with MRXDAV CCProjectZeroMembers
138	WontFix	----	2014-Oct-27	Microsoft	Windows-Kernel	forshaw	Windows: SMBv2 Symlink to Local File Vulnerability CCProjectZeroMembers
139	Fixed	----	2014-Oct-30	Adobe	Reader	mjurczyk	Adobe Reader X and XI for Windows out-of-bounds write in AGM.dll CCProjectZeroMembers
140	Fixed	----	2014-Oct-30	Adobe	Reader	mjurczyk	Adobe Reader X for Windows out-of-bounds read/write in CoolType.dll CCProjectZeroMembers
141	Fixed	----	2014-Oct-30	Adobe	Reader	mjurczyk	Adobe Reader X and XI for Windows object use-after-free in AcroForm.api CCProjectZeroMembers
142	Fixed	----	2014-Oct-30	Adobe	Reader	mjurczyk	Adobe Reader X for Windows out-of-bounds read in AGM.dll CCProjectZeroMembers
143	Fixed	----	2014-Oct-30	Adobe	Reader	mjurczyk	Adobe Reader X and XI for Windows out-of-bounds read in AcroRd32.dll CCProjectZeroMembers
144	Fixed	----	2014-Oct-30	Adobe	Reader	mjurczyk	Adobe Reader X and XI for Windows out-of-bounds write in CoolType.dll CCProjectZeroMembers
145	Fixed	----	2014-Oct-30	Adobe	Reader	mjurczyk	Adobe Reader X for Windows out-of-bounds write in AcroRd32.dll CCProjectZeroMembers