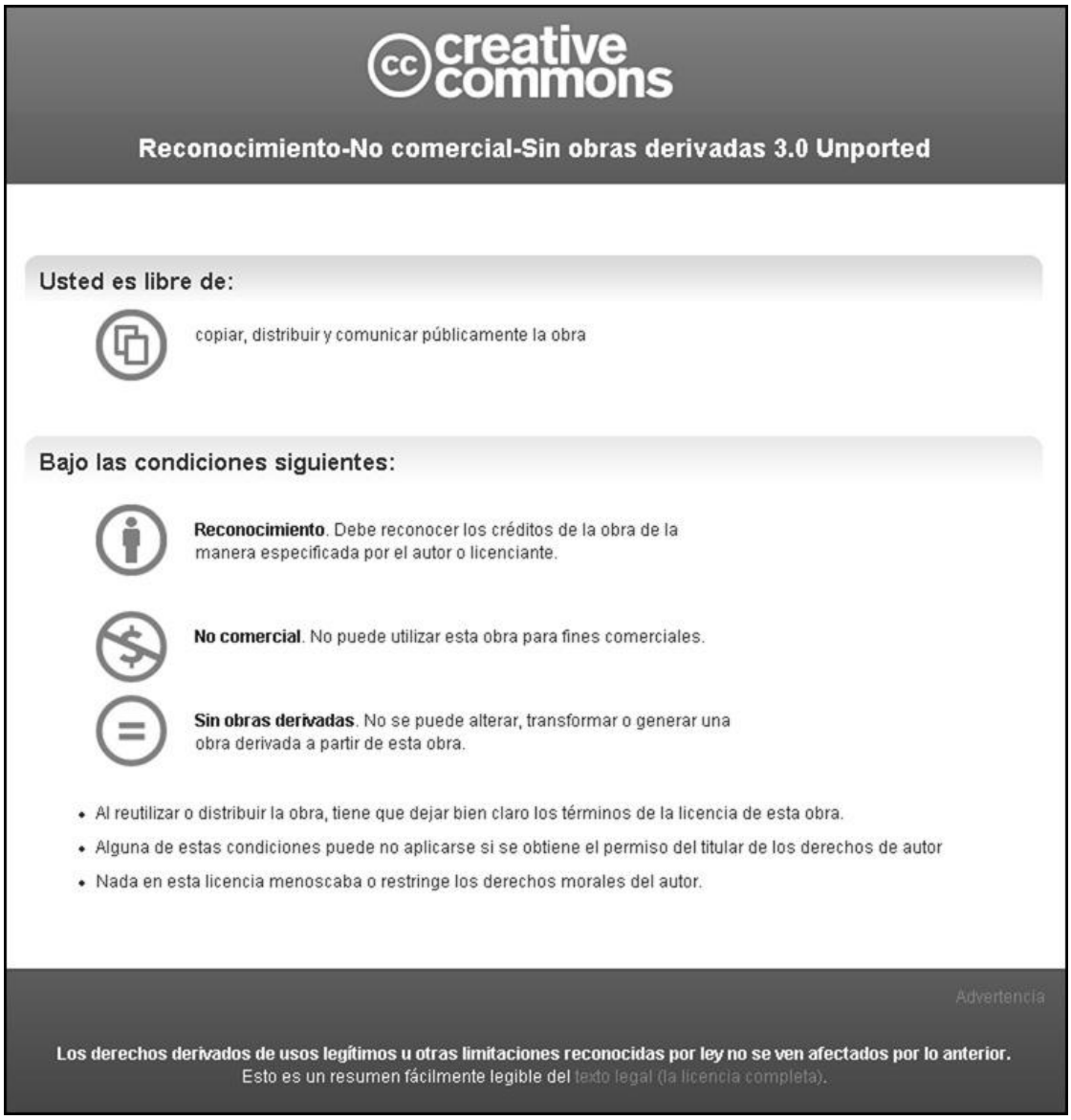
¿Cuánto tardan los grandes fabricantes de software en arreglar una vulnerabilidad?

Estudio sobre la demora de los fabricantes de software en la corrección de vulnerabilidades no públicas

Hispasec Sistemas

Septiembre 2009



Introducción

_ ¿Cuánto tardan los grandes fabricantes de software en arreglar una vulnerabilidad?

El tiempo que un fabricante tarda en hacer pública una solución para una vulnerabilidad es una de las métricas más importantes para conocer cómo maneja la seguridad. Suele existir cierta controversia en este aspecto. Se achaca a los fabricantes que tardan demasiado en disponer de una solución efectiva que ofrecer a sus clientes o usuarios. Mucho más cuando la vulnerabilidad es conocida y por tanto sus clientes "perciben" el peligro de utilizar ese software.

Existen dos escenarios muy diferentes a la hora de solucionar una vulnerabilidad: **que sea conocida públicamente, o que no**. Esto es determinante para los grandes fabricantes. En el segundo caso, el ritmo de solución es muy distinto al primero. Su imagen no está en entredicho, los clientes no se sienten en peligro... pueden tomarse la solución con más calma, y centrarse en asuntos mucho más urgentes (que seguro que existen). En Hispasec nos hemos preguntado **cuánto tardan los grandes fabricantes en solucionar una vulnerabilidad cuando no sufren la presión de los medios, cuando la vulnerabilidad es solo conocida por ellos y quien la ha descubierto.** Cómo reaccionan ante esta situación "ideal" (desde su punto de vista), en la que la vulnerabilidad les ha sido comunicada en secreto, y ambas partes acuerdan no hacerlo público hasta que exista una solución.

Este es un escenario relativamente sencillo de evaluar, puesto que podemos tomar la fecha en la que el fabricante fue informado como inicio del contador, y la fecha en la que se publica una solución como final. **El tiempo que haya transcurrido nos permitirá saber de forma precisa cuánto tardan los fabricantes en solucionar una vulnerabilidad que no es pública.** Nos hemos servido de iDenfense y ZeroDayInitiative para realizar un pequeño estudio al respecto.

_ iDenfense y ZeroDayInitiative

Son dos iniciativas de compañías privadas que compran vulnerabilidades, con la única condición de que se le cedan en exclusiva. La intención de estas dos empresas es apropiarse de vulnerabilidades relevantes en sistemas muy usados. Los investigadores privados que encuentren un fallo, pueden acudir a ellos a vender los detalles. Una vez pagan por la vulnerabilidad, estas dos empresas aplican la política de "revelación responsable", es decir, informan al fabricante del problema y anuncian el fallo (siempre que sea posible) solo cuando existe parche disponible. Ambas compañías esperan (a veces pacientemente) a que el fabricante haya solucionado la vulnerabilidad para hacer público su descubrimiento. Se centran en grandes empresas de software, y sobre ellas hemos realizado el estudio. También se centran en vulnerabilidades relevantes, que supongan un impacto real y que permitan realmente ser explotadas por un atacante.

_ Cómo se ha realizado el estudio

Una vez que la vulnerabilidad sale a la luz, tanto iDefense como ZeroDayInitiative publican una cronología de la vulnerabilidad, en la que ofrecen información sobre cuándo fue informado el fabricante, cuándo reconoció el fallo, y cuándo se estableció un fecha en la que ambos harían pública la vulnerabilidad (que normalmente es cuando existe parche). Si se da algún tipo de incidencia durante ese periodo (que el fabricante o descubridor necesite más información, se niegue a solucionarlo...) también queda reflejado en él.

Nos hemos servido de esa cronología para calcular cuánto tiempo necesita el fabricante para solucionar un fallo, desde que se le informa hasta que publica un parche. Pero bajo una condición muy importante: la vulnerabilidad no es pública. Se supone que solo el descubridor, la empresa intermediaria (iDefense y ZeroDayInitiative) y el fabricante la conocen. ¿Cómo actúan los fabricantes sin la presión de que el fallo sea público o esté siendo aprovechado activamente?

El tiempo que necesita el fabricante normalmente incluye:

* Reconocimiento y estudio de la vulnerabilidad
* Pruebas y alcance
* Programación del parche
* Pruebas de estabilidad, interoperabilidad y rendimiento del parche
* En el caso de que (como Oracle, Microsoft, y ahora Adobe) se siga la política de publicación de parches en unas determinadas fechas, se añade además esa diferencia de días hasta la fecha establecida.

Hemos identificado cada vulnerabilidad por su CVE. También hemos querido añadir el valor base del CVSS (versión 2) a cada una de ellas, para que se pueda apreciar la gravedad de la misma.

_ CVE

El CVE es el Common Vulnerabilities and Exposures, un estándar (administrado por la organización Mitre.org) que se encarga de identificar unívocamente a las vulnerabilidades. El CVE ha tenido gran aceptación entre todos los fabricantes porque la mayor parte de las veces es muy complejo saber a qué vulnerabilidad nos estamos refiriendo solo por ciertas características. Se hace necesario una especie de número de identidad único para cada fallo, puesto que en ocasiones son tan parecidas, complejas o se ha ofrecido tan poca información sobre ellas que la única forma de diferenciar la vulnerabilidad es por su CVE. Si no existe CVE del problema, lo hemos identificado por el CVE genérico CVE-000-000. Algunas vulnerabilidades están identificadas por un "CAN" en vez de "CVE". Se trata del formato "antiguo" que ya no es usado por Mitre.org.

En algunas ocasiones, incluso aunque contradiga el concepto, **varias vulnerabilidades pueden estar identificadas con un mismo CVE.** En estos casos lo que la identifica es el título asociado. Esto ocurre cuando una misma zona de código contiene varias vulnerabilidades, o ese mismo código genera varios fallos distintos. Los fabricantes en estos casos, a veces, agrupan varias vulnerabilidades dentro de un mismo CVE y lo solucionan todos a la vez, aunque hayan conocido el fallo en distintos momentos.

_ CVSS

CVSS (Common Vulnerability Scoring System), un estándar que gradúa la severidad de manera estricta a través de fórmulas establecidas. De esta forma los administradores conocerán de manera objetiva (a través de un número) la gravedad de los fallos. Está basado en los tres pilares de la seguridad de la información: la confidencialidad, integridad y disponibilidad de los datos, además de si el problema es aprovechable en remoto o local, la complejidad de explotación y la necesidad de estar autenticado en el sistema. Cuanto más próximo a 10, más grave es la vulnerabilidad.

_ Con qué criterio se han elegido las vulnerabilidades

Se han elegido todas las vulnerabilidades de cada fabricante, reportadas a iDefense y ZeroDayInitiative desde 2005 hasta final de agosto de 2009. Algunos fabricantes tienen cientos de vulnerabilidades y otros apenas unas decenas. **Esto no quiere decir absolutamente nada sobre la cantidad de vulnerabilidades que sufren sus productos, o que un producto sea menos vulnerable que otro.** Significa simplemente que se reportan menos a través de estos métodos, bien porque no interesen a los propios iDefense o ZeroDayInitiative, bien porque no interesen a los investigadores. **Evidentemente, por popularidad, el número de alertas de Microsoft Windows es significativamente mayor en este estudio. La cuestión es simple: se reportan más a través de estos métodos porque son las vulnerabilidades mejor pagadas.** Sin duda otros sistemas sufren de igual número de vulnerabilidades, pero al ser peor pagadas o interesar menos, no se reportan a través de iDefense o ZeroDayInitiative.

Según fabricante, el número de vulnerabilidades estudiadas que han sido reportadas desde 2005 a iDefense y ZeroDayInitiative son:

Fabricante	Número de vulnerabilidades estudiadas
Sun	36
Novell	41
HP	14
Microsoft	130
Apple	61
IBM	56
CA	36

Symantec	30
Oracle	16
Adobe	29

_ Mala interpretación de las cifras

Este estudio ofrece unas cifras. Las cifras adornan titulares y rellenan gráficas, pero no hay que olvidar que informan en un contexto. Por sí solas no siempre tienen valor. Hay que reconocer que es complicado realizar un estudio objetivo en este aspecto, pero lo hemos intentado en la medida de lo posible. **Los valores ofrecidos no pretenden más que ofrecer una noción de cuánto tarda un gran fabricante en solucionar un fallo que le ha sido reportado a través de iDefense o ZeroDayInitiative.** No podemos aventurarnos a opinar sobre cuánto tarda en solucionar fallos que son reportados por otras vías, puesto que muchas de las vulnerabilidades solucionadas por los fabricantes son descubiertas por su propio equipo, y rara vez confiesan desde cuándo llevan trabajando en ellas.

Por tanto advertimos que estas cifras que ofrecemos pretenden ser rigurosas en la medida de lo posible (nos disculpamos por adelantado ante cualquier error no intencionado o errata que este estudio pueda contener), y darnos una idea global de cuánto necesita un gran fabricante para solucionar un fallo de seguridad sin la presión de que la vulnerabilidad sea conocida. **No se calcula en ningún momento, la celeridad de un fabricante cuando la vulnerabilidad es conocida y está siendo aprovechada,** pues como hemos indicado, son dos escenarios muy distintos en los que los fabricantes actúan de forma muy diferente a la estudiada.

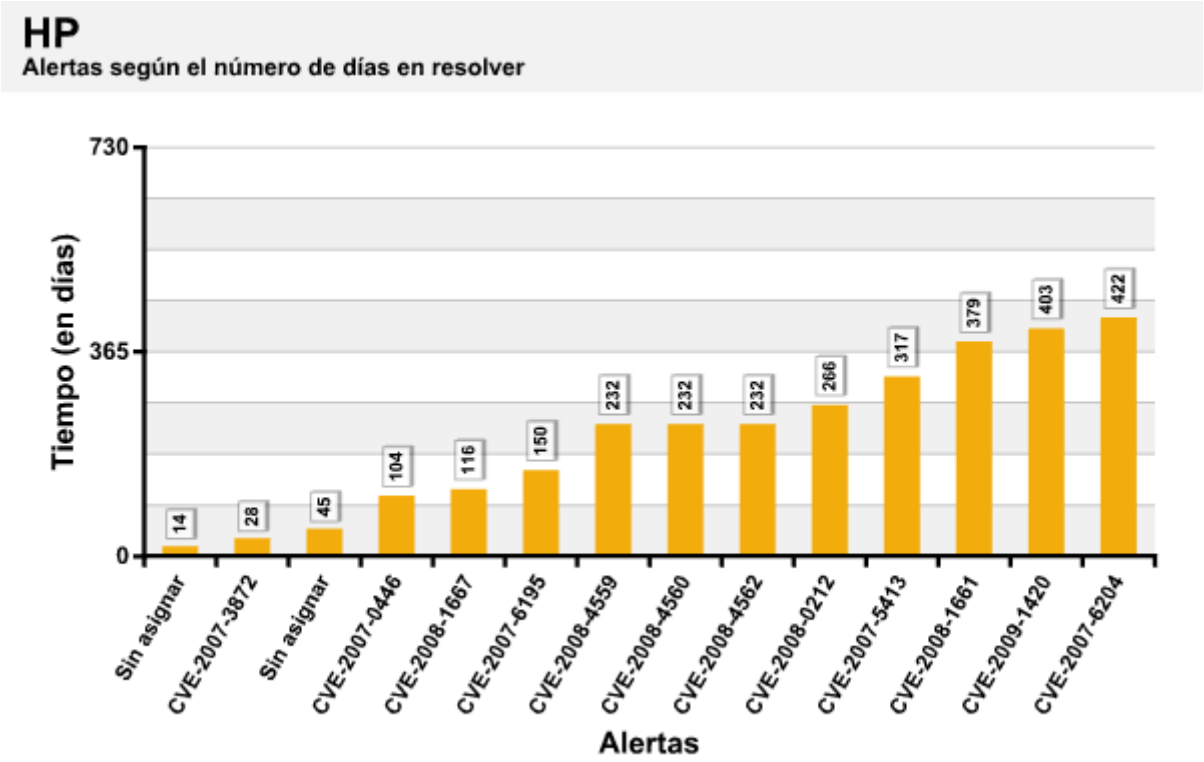
_ Coeficiente de variación

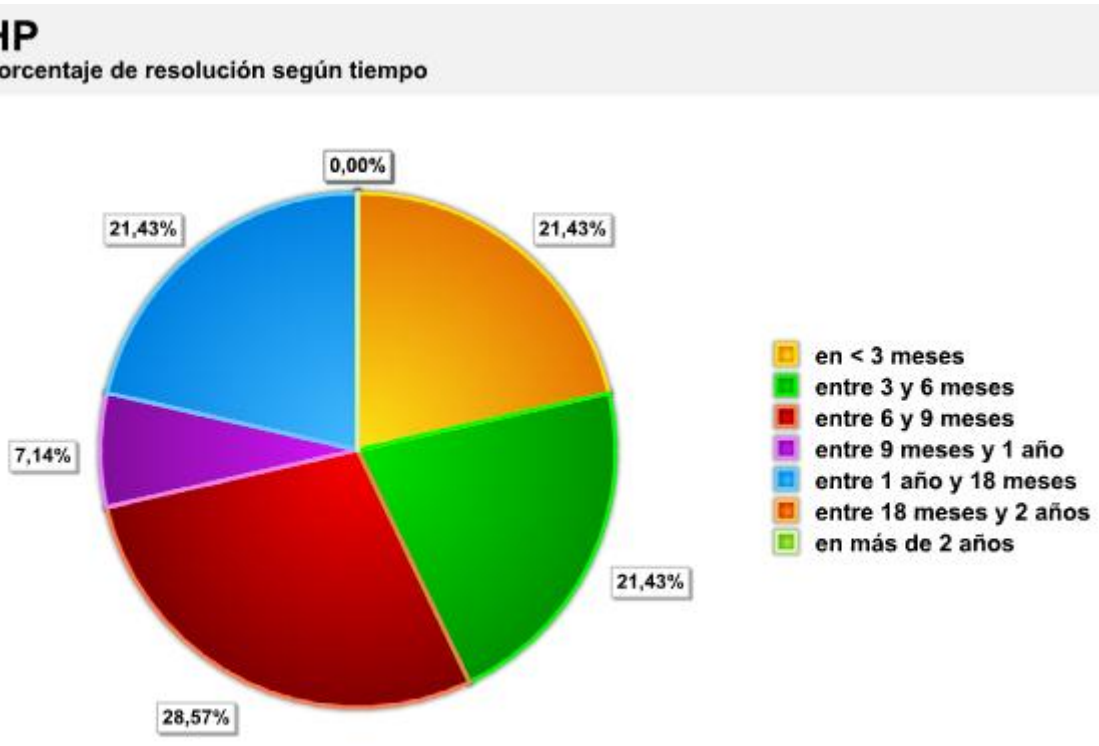
Al realizar un estudio estadístico en dos poblaciones diferentes, la media puede llegar a ser muy engañosa. Esta circunstancia es aprovechada en otros estudios como arma de doble filo. No queremos caer en esa trampa. Ya se sabe que si dos personas comparten un pollo para comer, pero una de ellas se lo come todo, según la media estadística ambas habrían comido la mitad. Es necesario conocer la media y el grado de dispersión, para no llevarse a engaño. Al calcular una media sobre 20 objetos, un par de valores muy elevados pueden, por ejemplo, "contaminarla". Así que para eso se calcula el coeficiente de variación. Cuando existen varias poblaciones, no podemos acudir a la desviación típica para ver la mayor o menor homogeneidad de los datos, sino a otro parámetro llamado coeficiente de variación y que se define como "el cociente entre la desviación típica y la media".

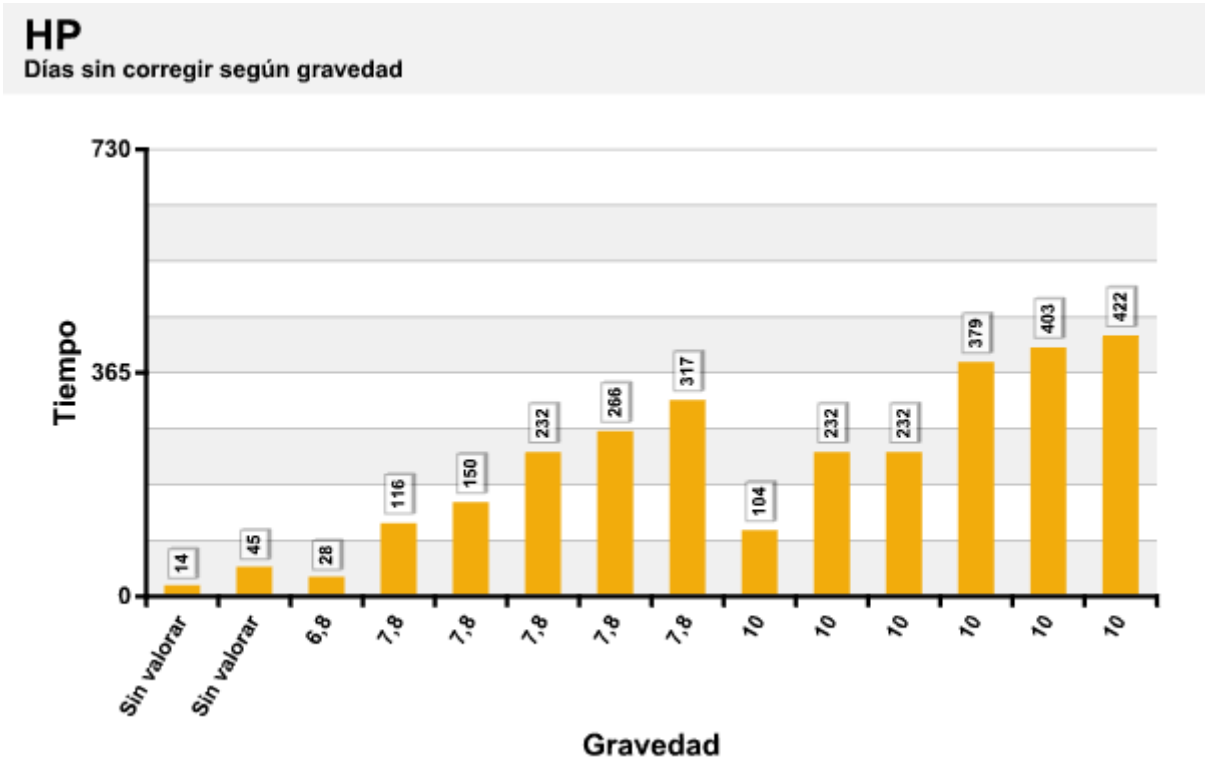
El coeficiente de variación es la división entre la desviación típica y la media, que nos dice el grado de dispersión. **Lo importante es saber que cuanto mayor sea, más dispersos son los resultados de la media. Por el contrario, cuanto más pequeño el valor, más homogéneos los valores.** Un coeficiente de variación mayor que 1 indica la presencia de algunos valores erráticos en la muestra que pueden tener una gran influencia en la estimación. La media no sería muy representativa en estos casos.

Hewlet Packard (HP)

14 vulnerabilidades estudiadas.





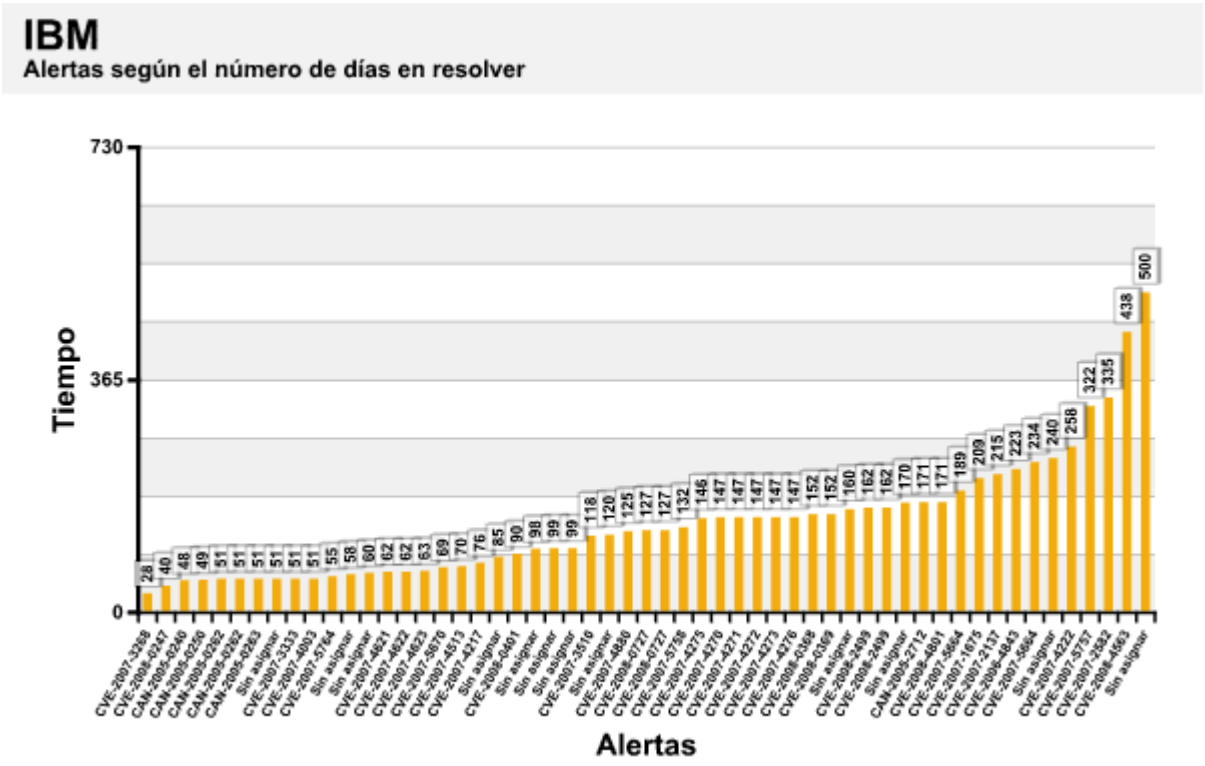


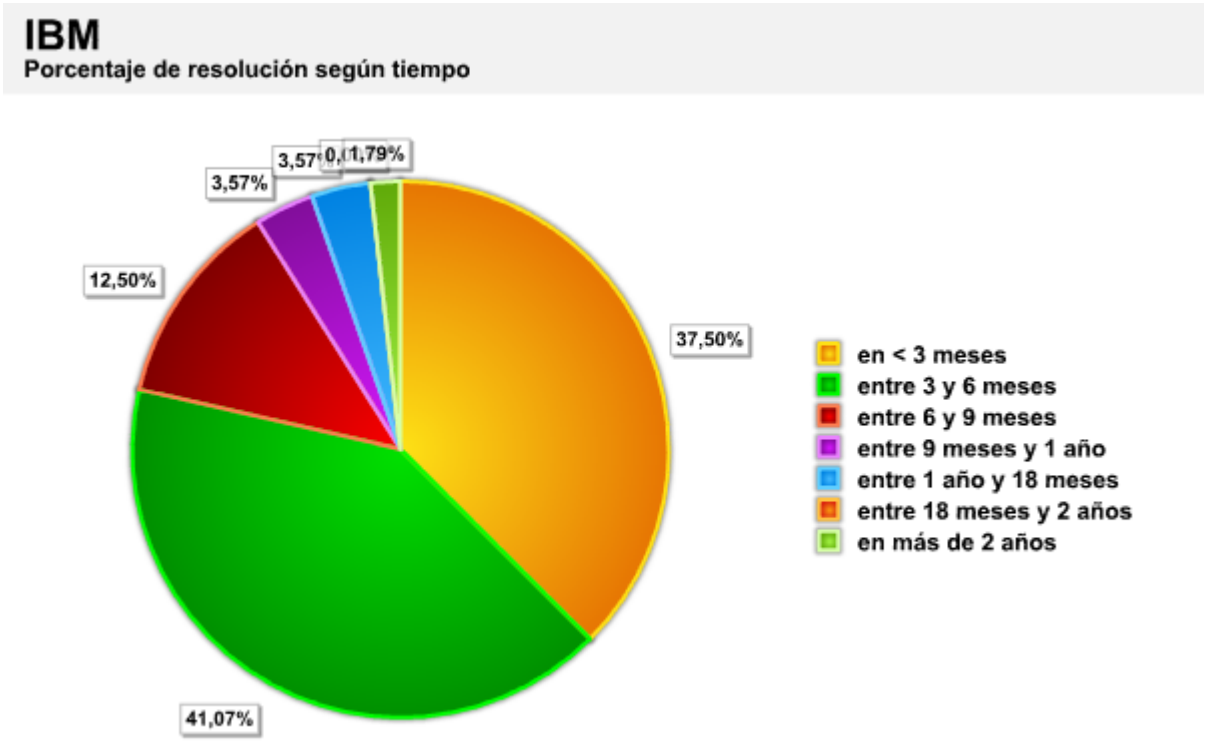
_ Curiosidades:

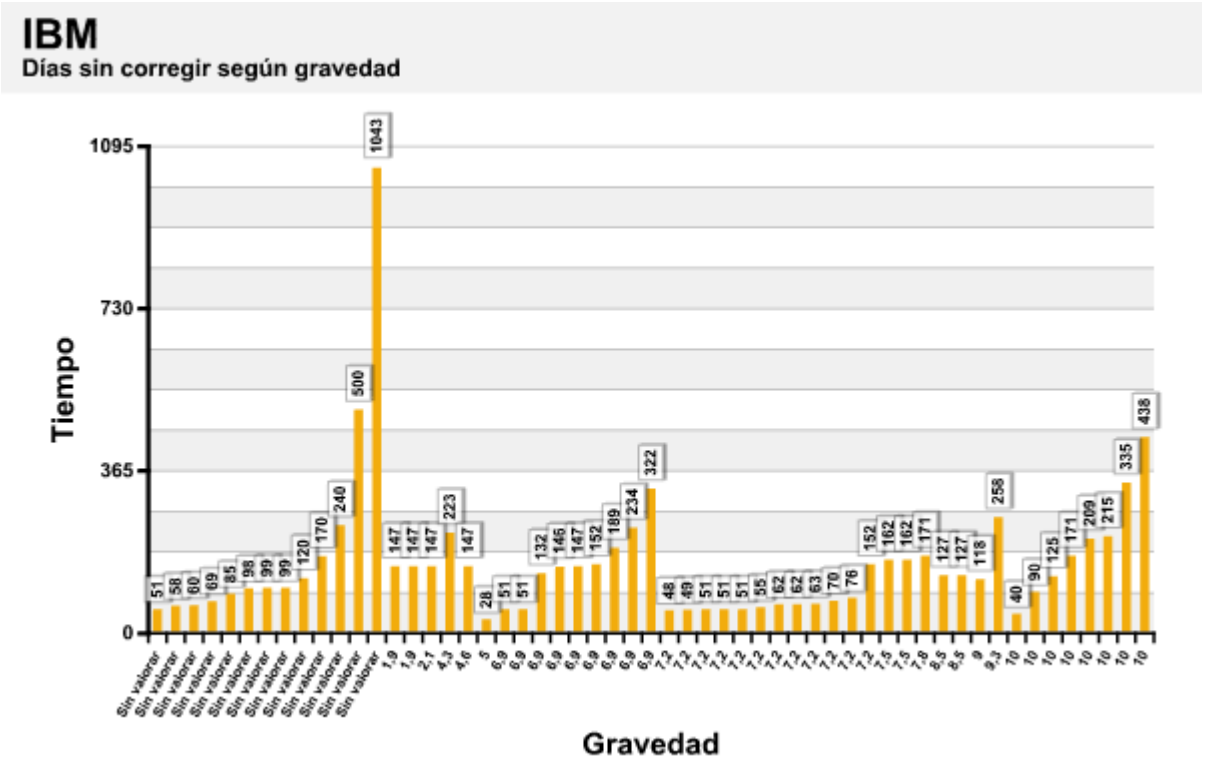
Una de las vulnerabilidades de HP que carece de CVE es un claro ejemplo de los problemas que pueden ocurrir si un fabricante no se da prisa a la hora solucionar un fallo, aunque este no sea público. El problema fue reportado a HP el 16 de febrero de 2007, pero muy poco después otros investigadores, con no muy buenas intenciones, descubrieron el fallo por su cuenta e hicieron público un exploit para aprovecharlo. HP se vio obligada a priorizar esta vulnerabilidad y hacerla pública antes de lo planeado (solo tardaron 45 días, una variación importante con respecto a su media).

Existen dos "curiosidades" con HP que nos parecen significativas, pero que no están incluidas en el informe. iDefense esperó durante casi 3 años a que solucionase un fallo en el componente ldcconn de HP-UX 11.11i. Pero HP no lo hizo, (a pesar de la insistencia de iDefense) puesto que alegaba se trataba de un producto que había dejado de ser soportado por HP en 2002 (aunque venía incluido en productos que se estaban usando activamente aún). Al final, HP no cedió y el fallo sin parche tuvo que hacerse público. Exactamente lo mismo ocurrió con el comando pfs_mountd.rpc de HP-UX.

56 vulnerabilidades estudiadas







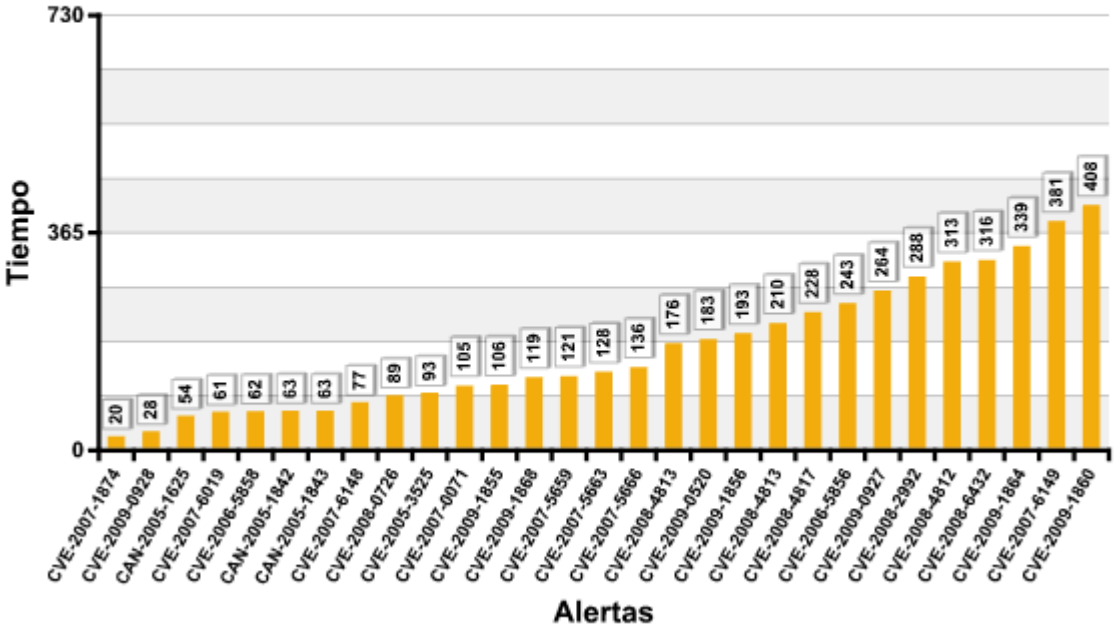
_ Curiosidades:

IBM y su sistema operativo profesional más extendido, AIX, destacaba en 2002 por el número de parches publicados, que semanalmente podía llegar a superar los 30. Hoy en día ese número se ha reducido sustancialmente, pero incluso para vulnerabilidades conocidas que afectan a componentes comunes de algunos sistemas operativos, AIX suele ir por detrás a la hora de solucionarlas.

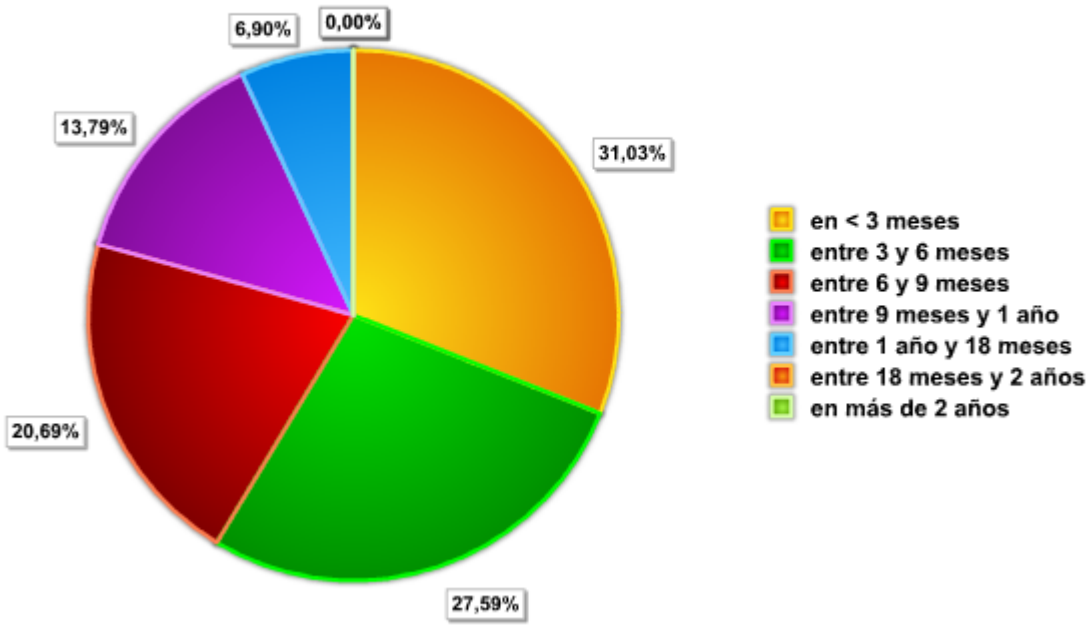
Adobe

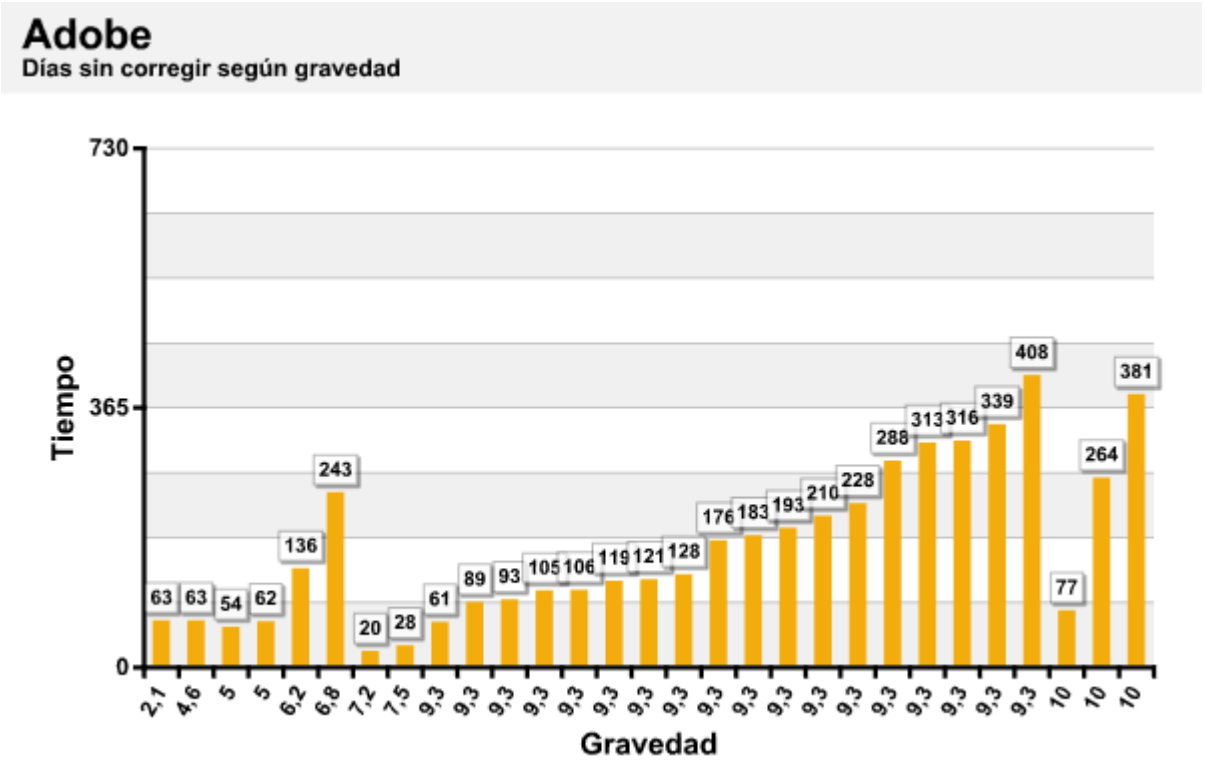
29 vulnerabilidades estudiadas.

Adobe
Alertas según el número de días en resolver



Adobe
Porcentaje de resolución según tiempo





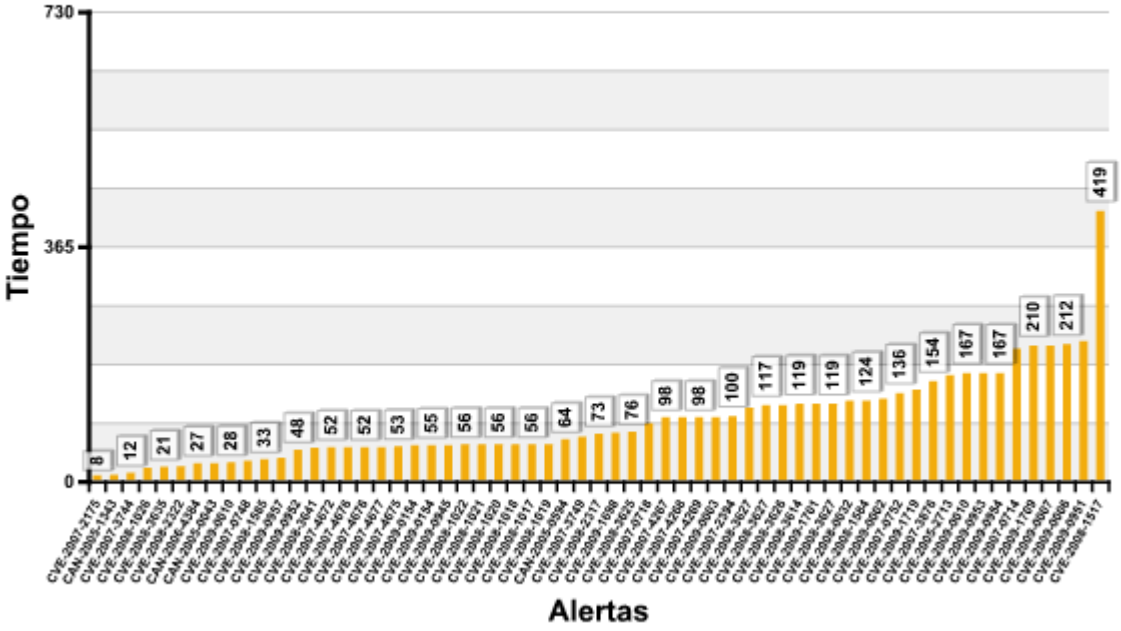
_ Curiosidades:

Algunas vulnerabilidades de Adobe se han solucionado "extraordinariamente" rápido para su media, pero esto tiene una explicación. En febrero se encontraron varios fallos en JBIG2 que permitían la ejecución de código a través de un archivo PDF y empezaron a ser aprovechados activamente por atacantes. Adobe, desde entonces, ya tenía sus ojos puestos en esa función. Pero no solo Adobe... los investigadores privados comenzaron también a encontrar nuevos y diferentes errores en ese mismo punto del código. Así que Adobe decidió solucionarlos todos de una sola tacada. La vulnerabilidad CVE-2009-0928, es uno de los múltiples fallos encontrados en la funcionalidad JBIG2 de PDF y Adobe tardó "solo" 28 días en arreglarlo porque, en realidad, ya venía trabajando en ese punto del código desde hacía mucho más tiempo y de forma más intensa (había un exploit público y los atacantes lo estaban aprovechando).

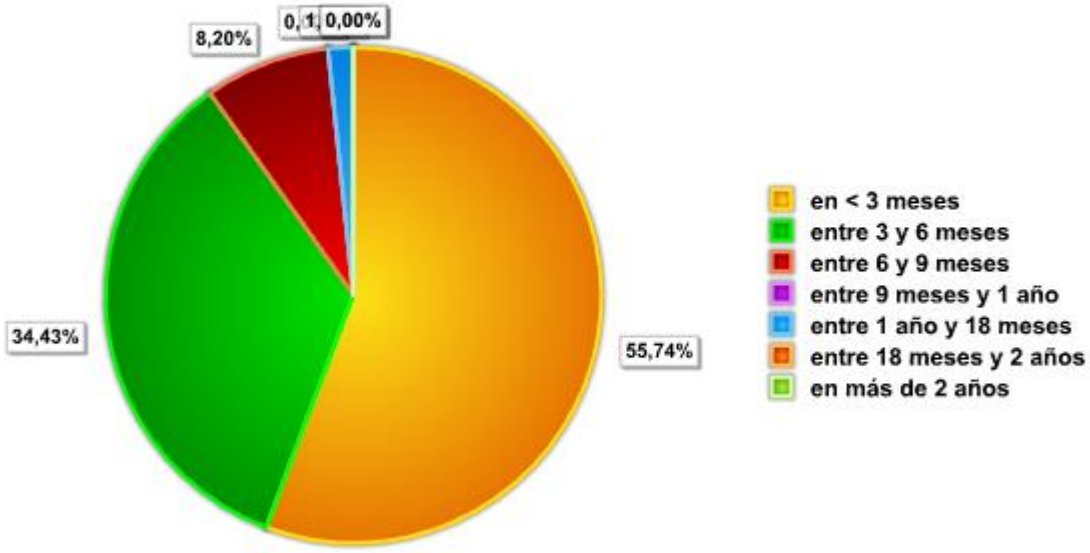
Apple

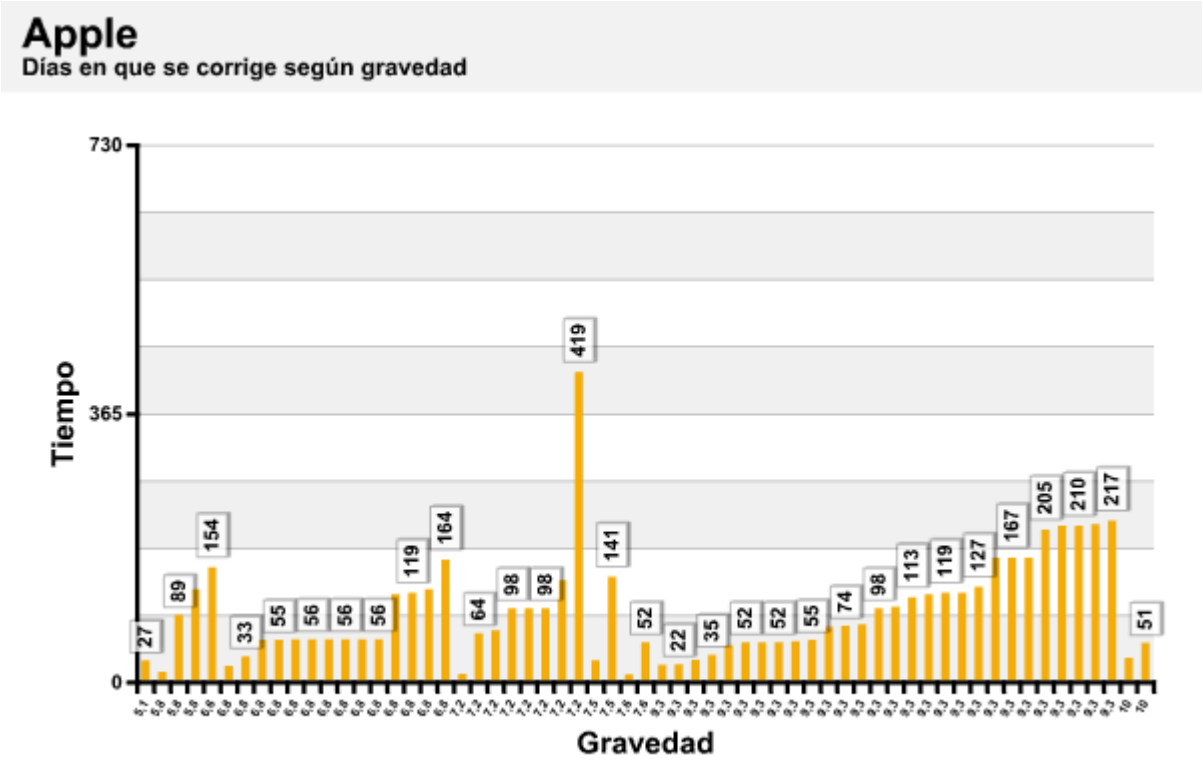
61 vulnerabilidades estudiadas.

Apple
Alertas según el número de días en resolver



Apple
Porcentaje de resolución según tiempo

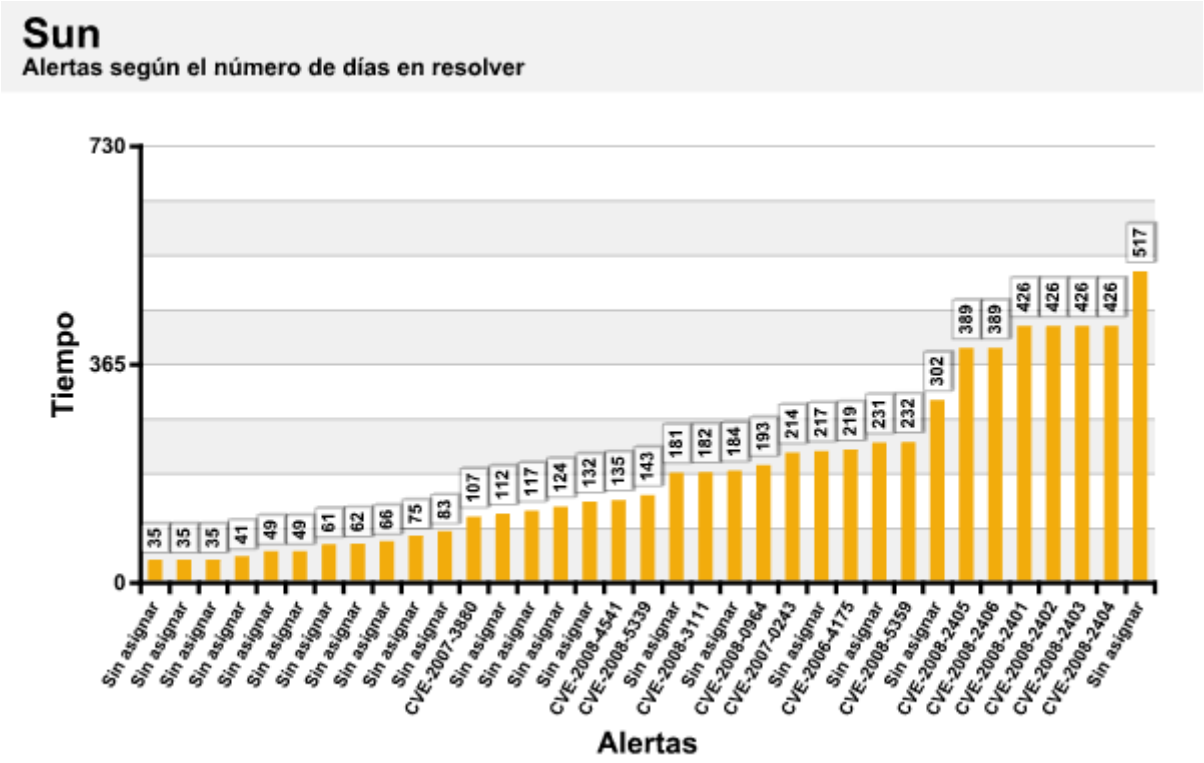


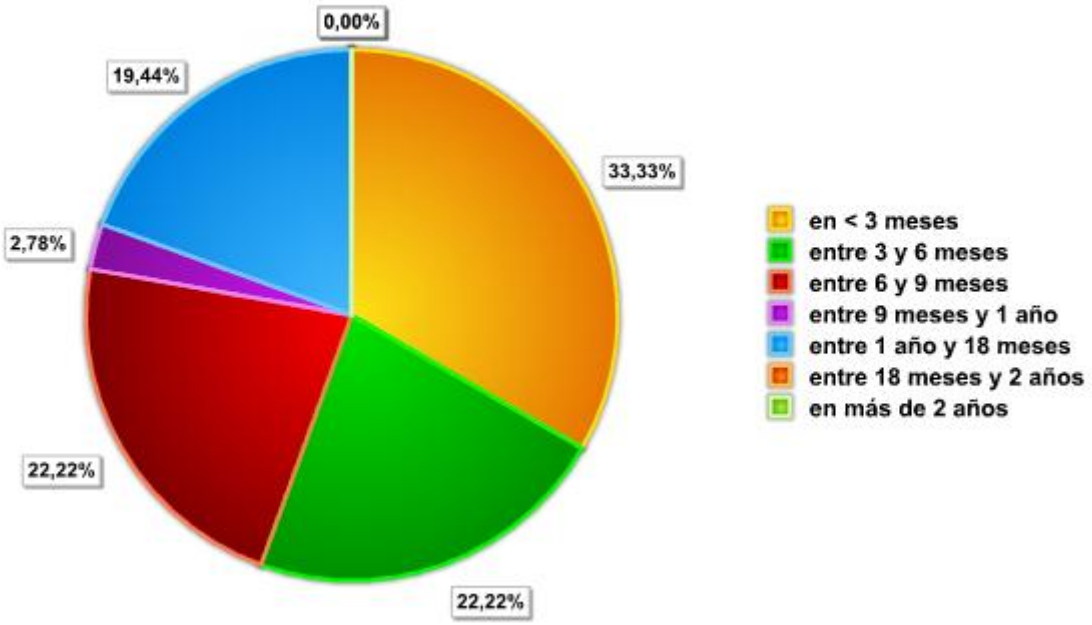


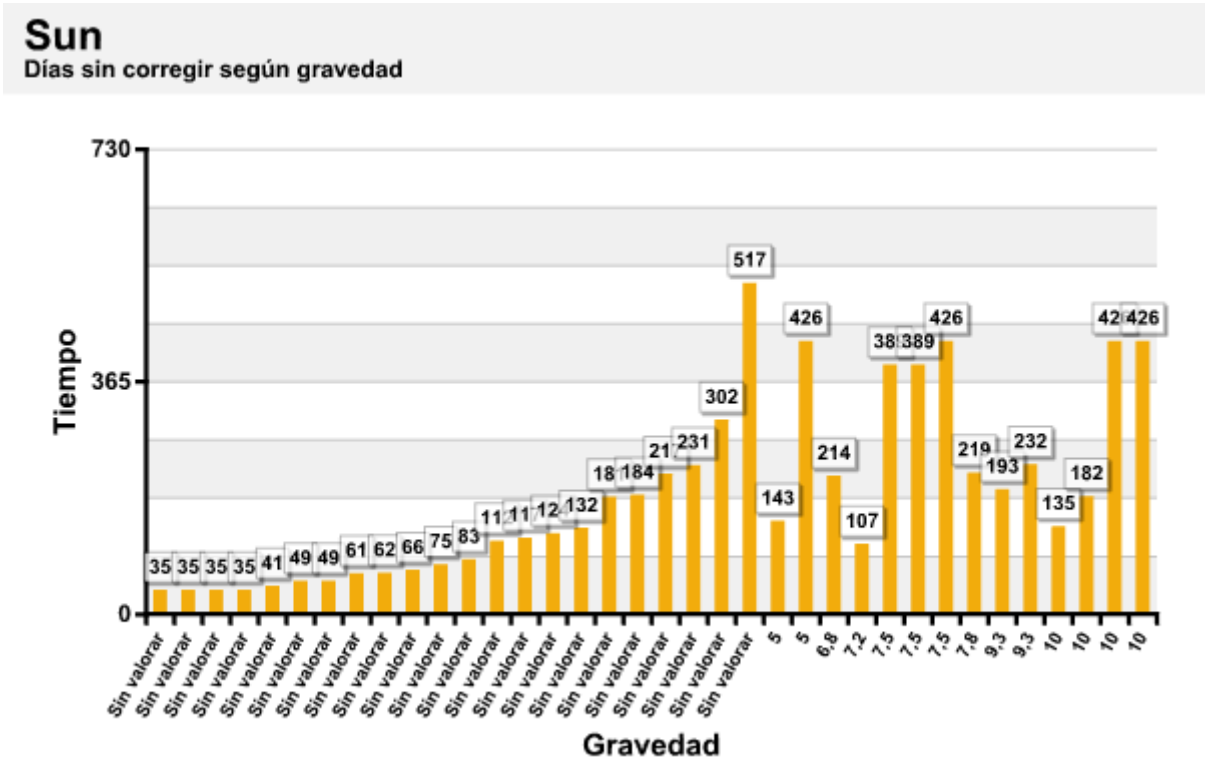
_ Curiosidades:

Aunque la media no lo represente, puntualmente Apple ha ido casi siempre por detrás a la hora de solucionar fallos de seguridad muy significativos en un tiempo razonable. En la macro-actualización de Mac OS X de mayo de 2009, se corrigieron 67 vulnerabilidades, pero dejaron sin solución un grave problema en el JRE (Java Runtime Environment) que podía ser aprovechado por atacantes para ejecutar código con solo visitar una página web. En 2008 con la vulnerabilidad en el protocolo DNS descubierta por Kaminsky, Apple fue el último en publicar un parche. Todos los grandes (Microsoft, Cisco, BIND...) sacaron el 8 de julio una solución coordinada a un problema que se había mantenido en secreto desde principios de año. Pero Apple no. Dejó a los usuarios de Mac OS X sin solución hasta casi tres semanas después. Igual con el fallo común de implementación de TCP, conocido como “socktress”, que Cisco, Microsoft, Check Point... solucionaron en septiembre de 2009. Curioso pues, que tarde menos en resolver vulnerabilidades reportadas de forma privada que las que son públicas. Como demuestran las gráficas, solo una vulnerabilidad le ha llevado más de un año.

36 vulnerabilidades estudiadas.



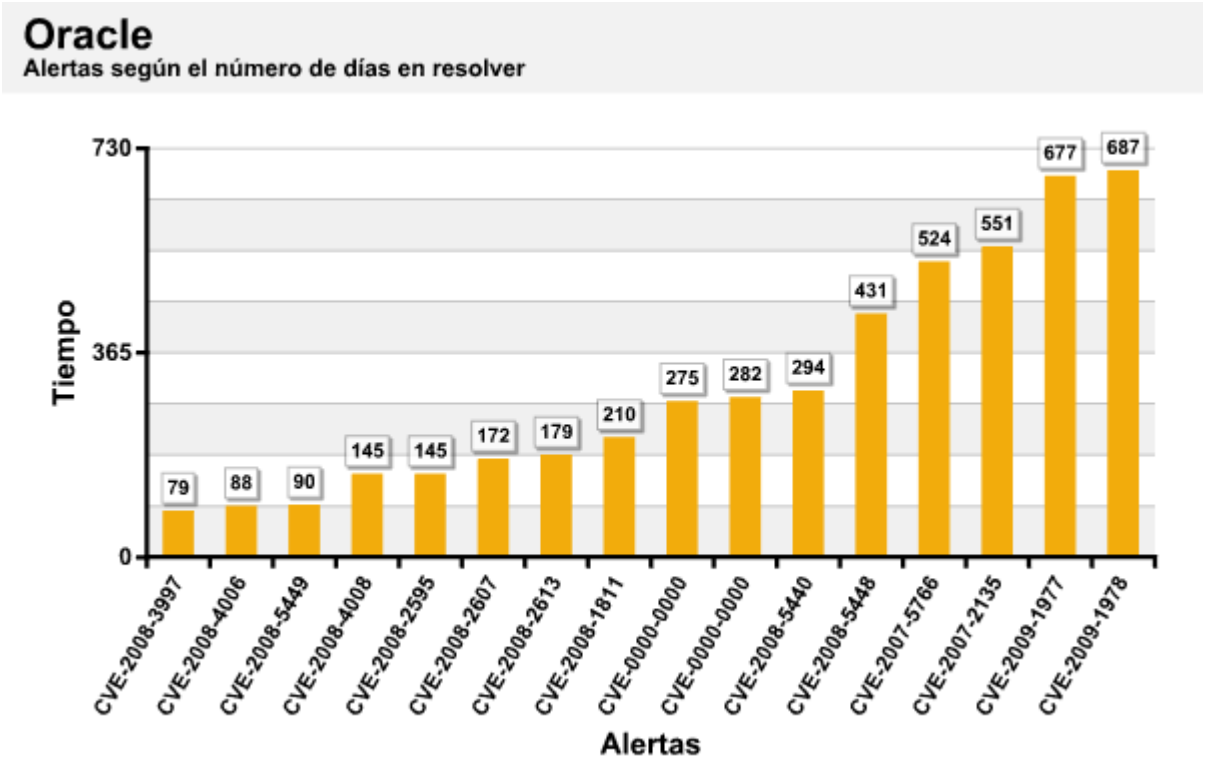


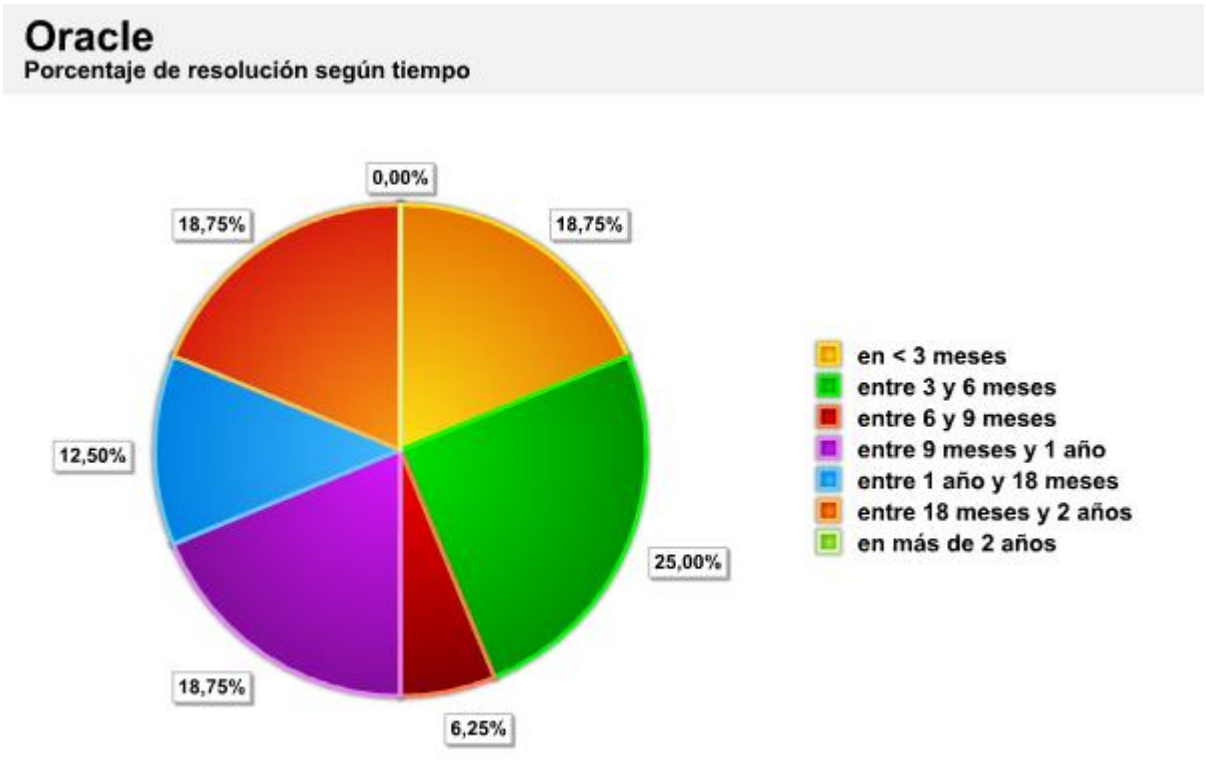


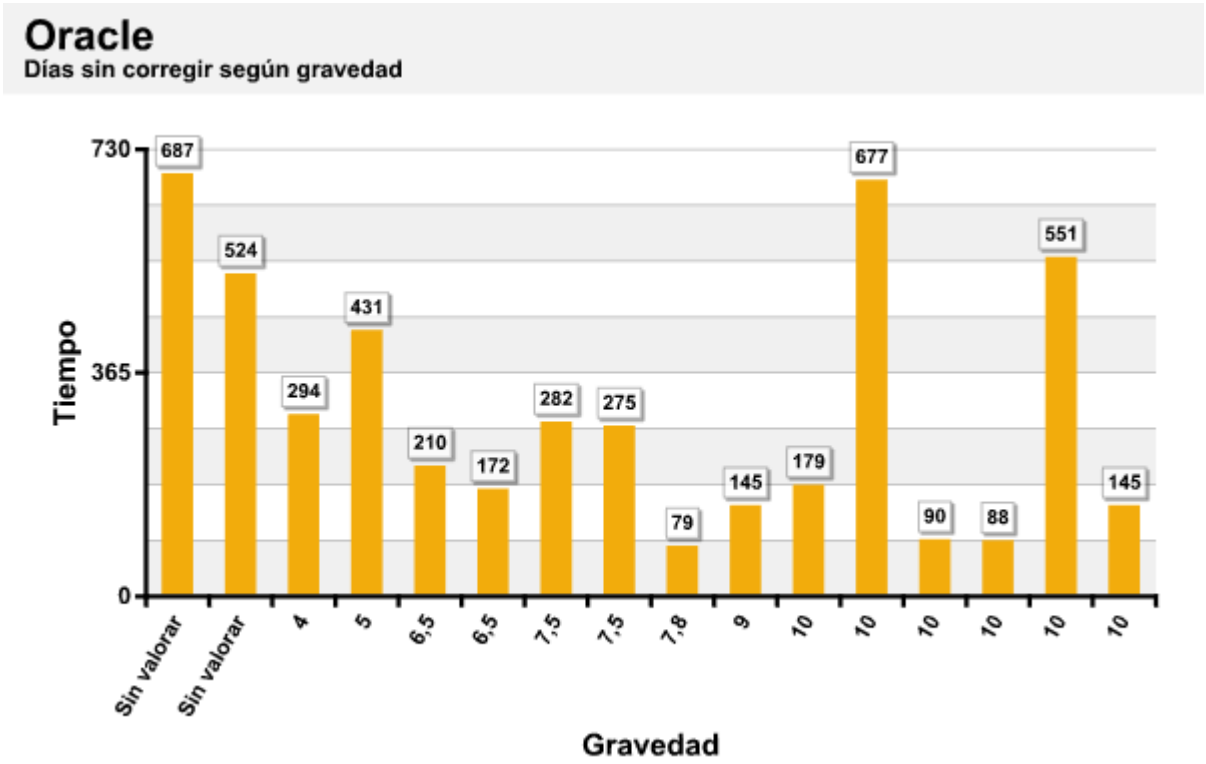
_ Curiosidades:

Sun suele tomarse su tiempo para solucionar vulnerabilidades en sus sistemas operativos Solaris. Incluso cuando los fallos son conocidos y públicos, puede dejar pasar años hasta que publica parche oficial. Además, por desgracia un importante porcentaje de sus parches producen inestabilidad en el sistema.

16 vulnerabilidades estudiadas.





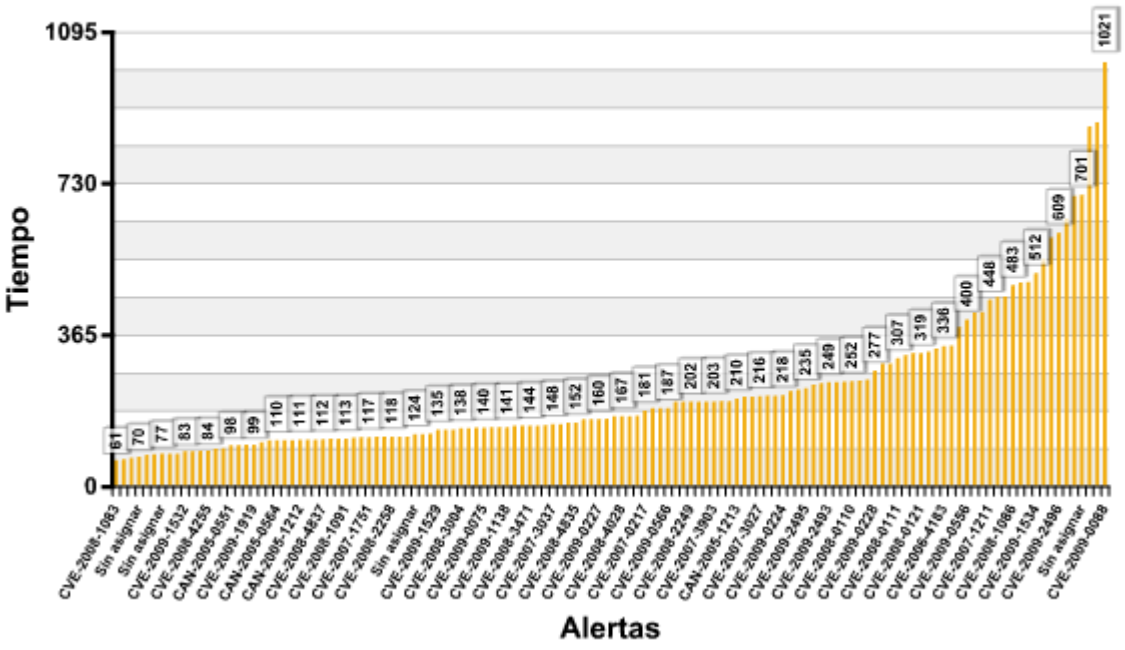


_ Curiosidades:

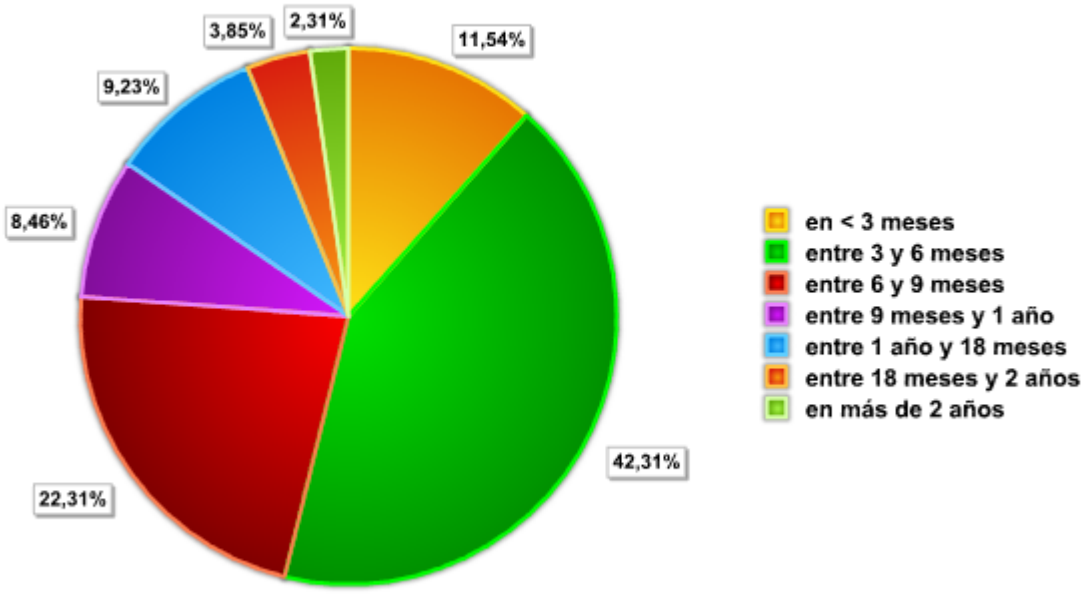
Sin duda Oracle ha sido el peor parado en este estudio, y no sin razón. Desde siempre, ha tenido serios problemas para administrar la seguridad de sus múltiples productos. A pesar de sus esfuerzos para mejorar su política de seguridad, no ha conseguido gestionar eficazmente las vulnerabilidades descubiertas, y ha sido duramente criticado por "abandonar" a sus clientes con vulnerabilidades públicas, explotadas, reconocidas y graves. En 2004, pasó 8 meses sin solucionar 34 vulnerabilidades conocidas. Paradójicamente, a finales de 2001 Internet se llenó de anuncios y banners que prometían que la nueva versión de Oracle era irrompible. Entre la comunidad, este mensaje perteneciente a una agresiva campaña de marketing no pudo más que tomarse a broma. No tardaron en aparecer todo tipo de desbordamiento de memorias intermedias, fallos remotos, locales, internos, exploits... algunos inclusos obvios y triviales. El software de Oracle seguía siendo vulnerable a todo tipo de fallos de seguridad, tanto o más que sus predecesores y, con el tiempo se está demostrando, menos que sus sucesores.

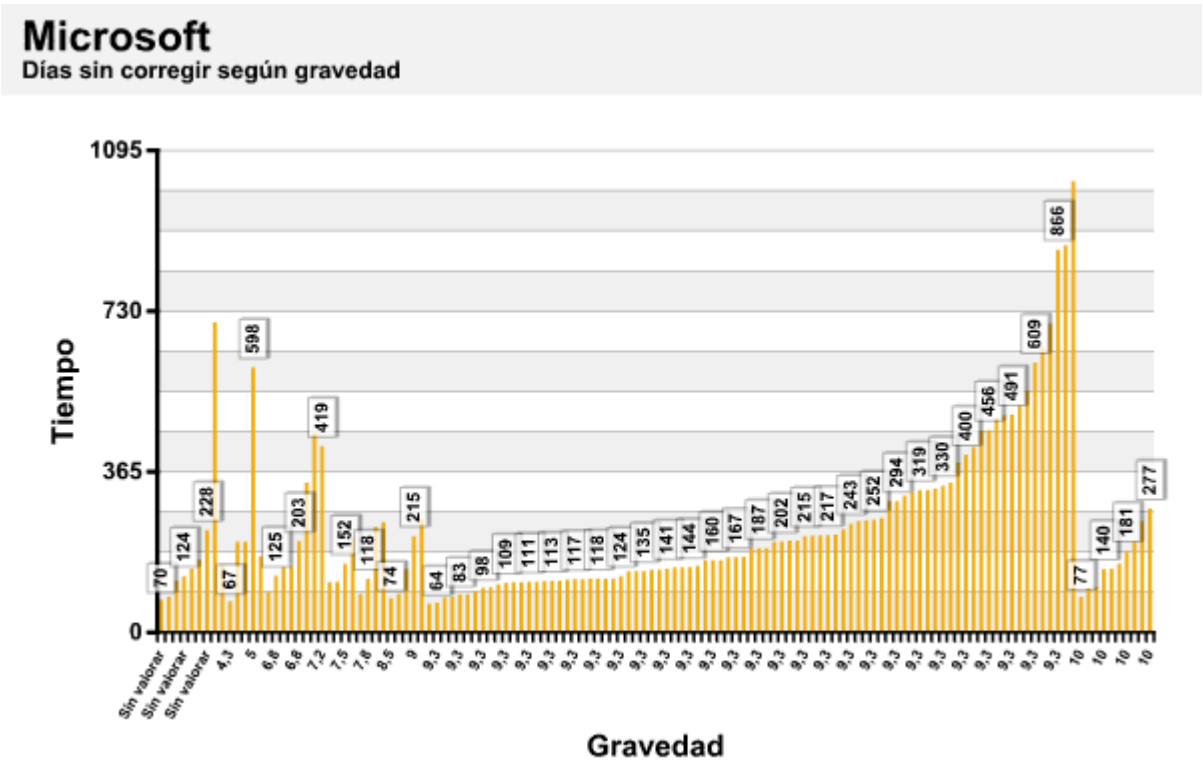
130 vulnerabilidades estudiadas.

MS
Alertas según el número de días en resolver



Microsoft
Porcentaje de resolución según tiempo





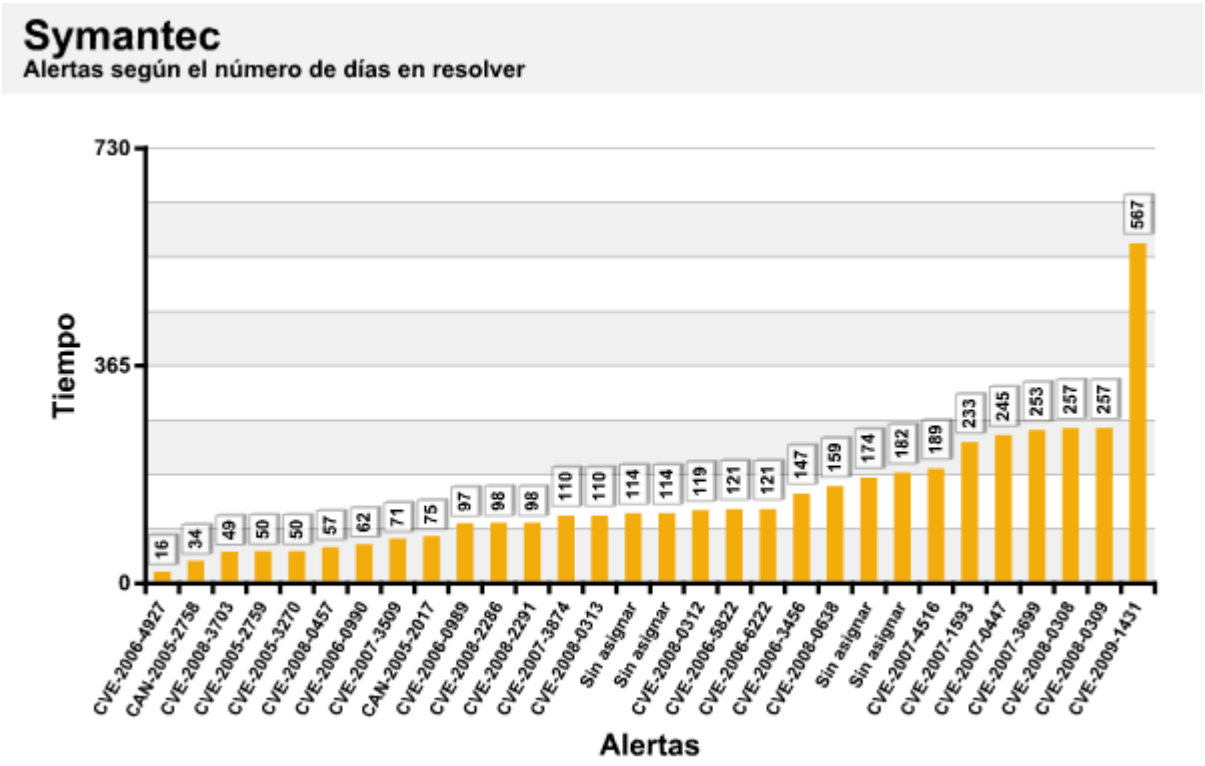
_ Curiosidades:

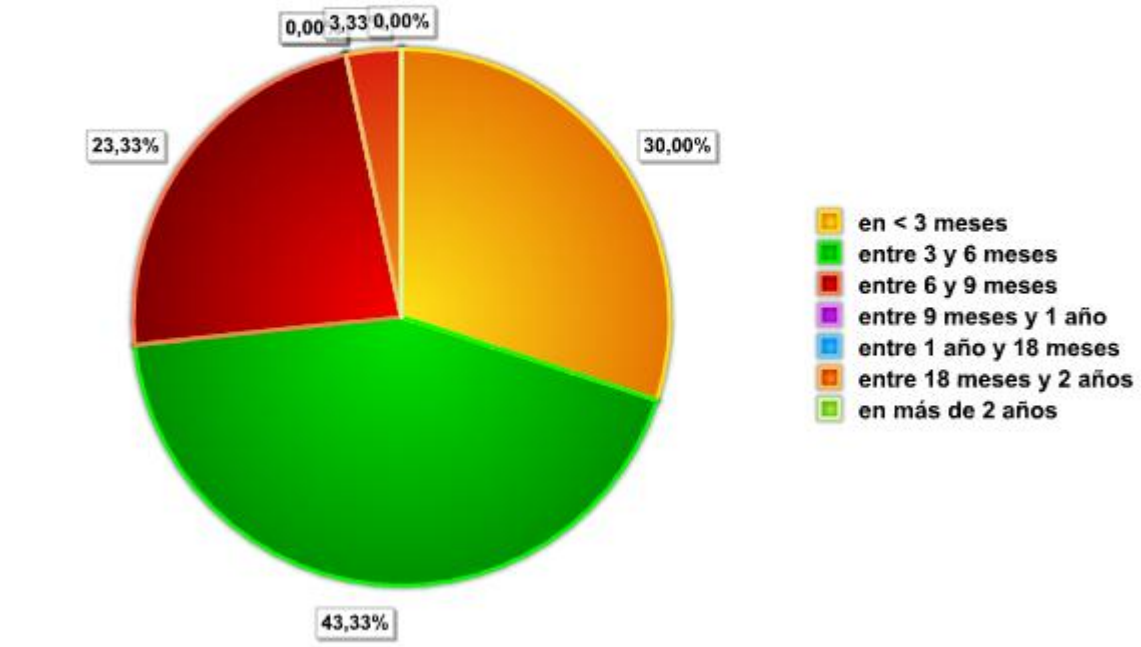
Microsoft ha mejorado infinitamente su política de seguridad desde, aproximadamente, 2004. Aun así (o quizás a causa de) sufre tremendos problemas para gestionar el problema de seguridad que acarrea desde sus inicios. Un desastroso planteamiento de la seguridad en sus primeros productos y la necesidad de compatibilidad hacia atrás, está haciendo que arrastre problemas de seguridad gravísimos que los atacantes saben aprovechar. Su enorme popularidad lo hace apetitoso objetivo de atacantes, y sin duda es el sistema con más vulnerabilidades reportadas a través de iDefense y ZeroDayInitiative, no en vano son las mejores pagadas. Esto, unido a la gran cantidad de productos y sistemas y la gran interoperatibilidad que existe entre ellos, hace que cada parche deba ser mirado con lupa antes de su publicación para que la estabilidad quede más o menos garantizada. Tampoco hay que olvidar que Microsoft es sorprendida con problemas de seguridad "0-day" varias veces al año, con lo que debe priorizarlos y solucionarlos cuanto antes, cosa que a veces consigue y otras no tanto. En general, se toma "con calma" los fallos de seguridad que les son reportados de forma privada, aunque en ocasiones esto es un arma de doble filo.

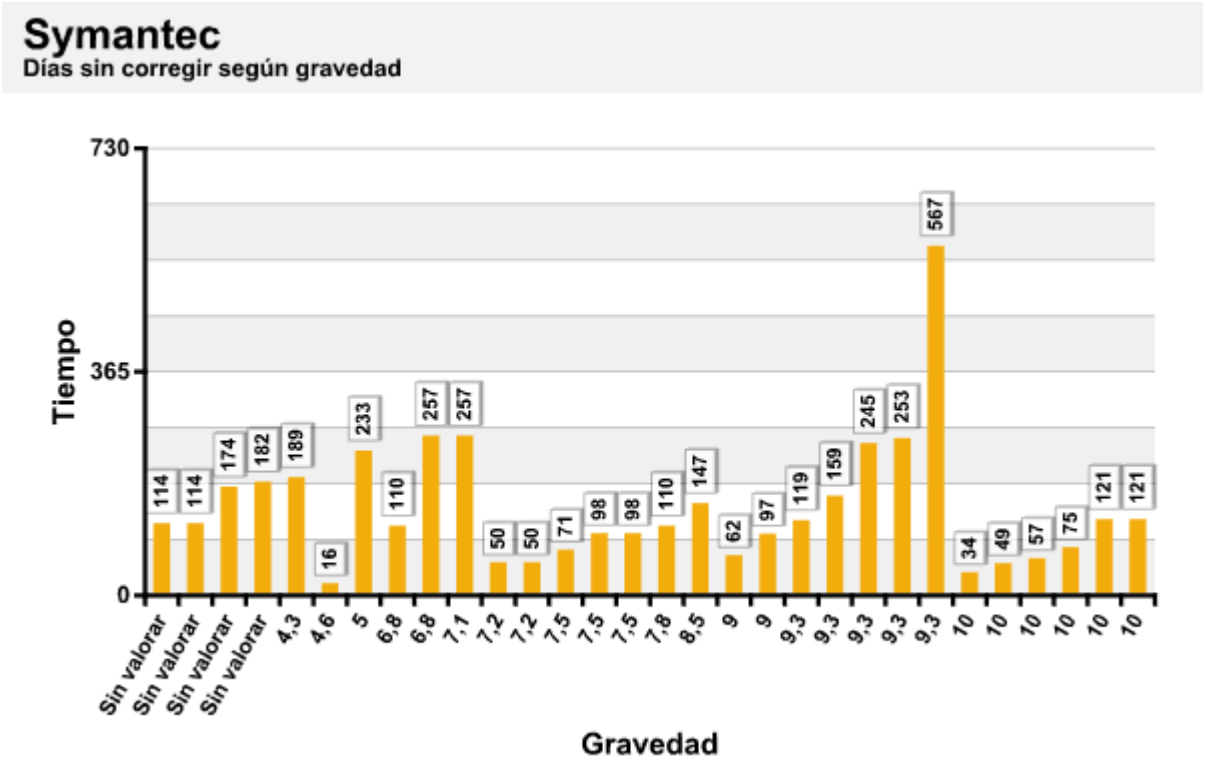
La compañía se vuelca totalmente en un fallo cuando es público, si no, va a "otro ritmo" a la hora de parchear. Incluso cuando la vulnerabilidad es pública, hay que tener en cuenta que Microsoft hace insistentes pruebas de compatibilidad cada vez que saca un parche, y aun así, a veces comete errores. El código del sistema operativo es demasiado complejo y las interacciones pueden ser impredecibles, así que la estrategia para los parches de Windows es "lento pero (en lo posible) seguro". En una de las últimas vulnerabilidades corrgidas (CVE-2008-0015), se le adelantaron los atacantes. Microsoft conocía el fallo (lo descubrieron internamente) desde la primavera de 2008, pero no fue hasta principios de julio de 2009 que sacó un parche, porque otros atacantes la descubrieron independientemente, y comenzaron a aprovecharla para ejecutar malware en los sistemas. En ese momento Microsoft dedicó todos sus recursos a solucionarlo, y dispuso del parche en apenas unos días (llevaba trabajando en él un año). Este fallo no ha sido reflejado en este estudio porque no fue reportado a través de iDefense o ZeroDayInitiative.

Destaca en Microsoft la vulnerabilidad CVE-2009-0088, por esperar 1021 días (tres años) en solucionarla. Esto puede tener su explicación en que el fallo solo afecta a Microsoft Office 2000 y XP, productos de los que Microsoft, "ya no se preocupa tanto". Sin embargo, es curioso como otros fallos en Office (también afectando a 2000 y XP) son solucionados en "apenas" 6 meses.

30 vulnerabilidades estudiadas.





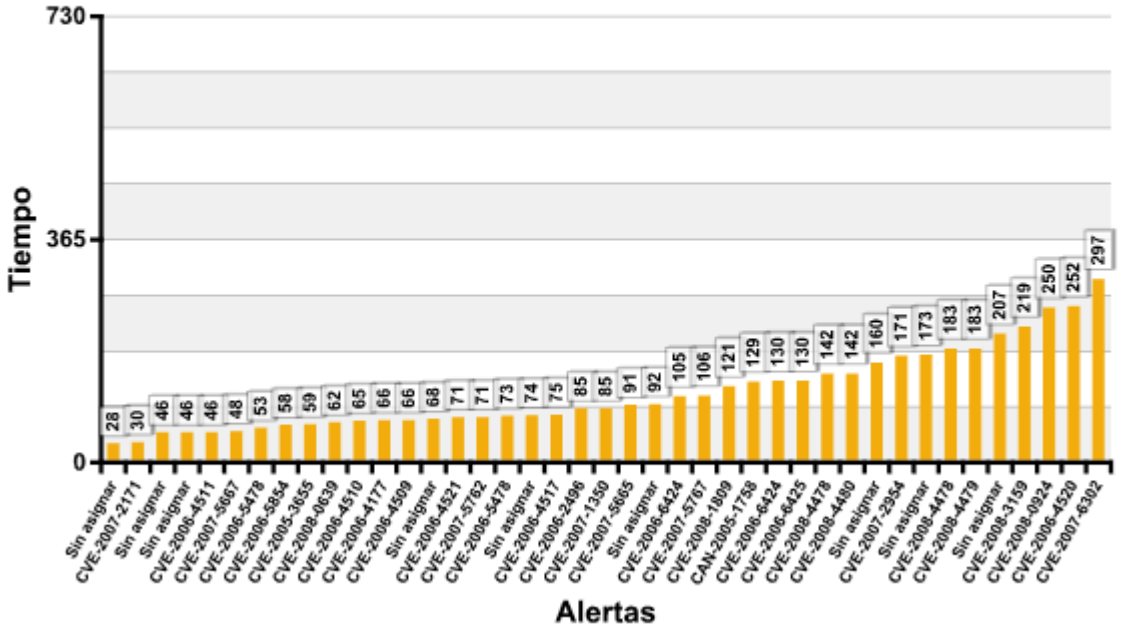


_ Curiosidades:

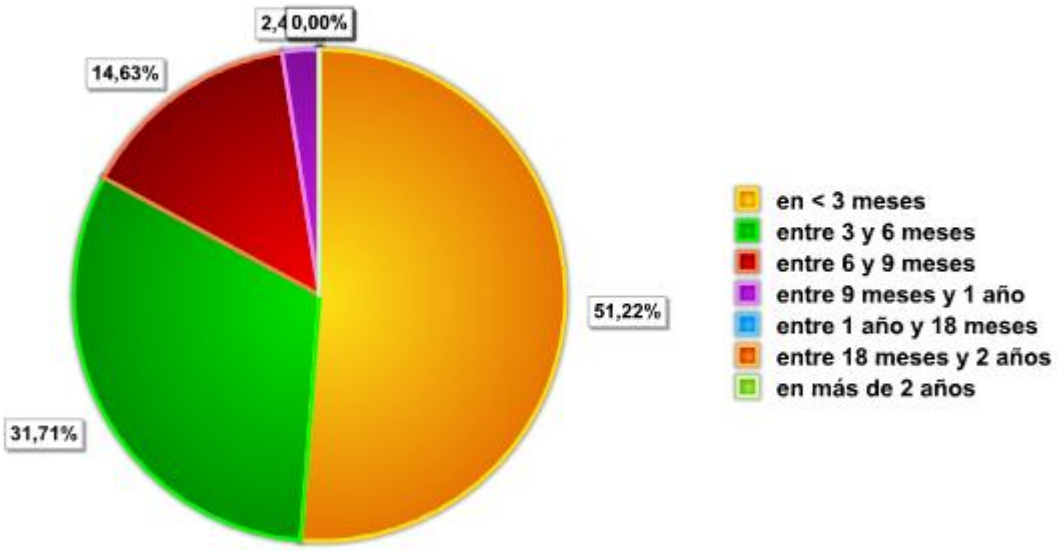
Destaca la vulnerabilidad CVE-2009-1431 en Symantec System Center de Symantec, sin solucionar desde octubre de 2007 hasta marzo de 2009. El origen de la vulnerabilidad era un fallo de diseño que, de ser cambiado, modificaría sustancialmente la forma de comportarse del programa. Symantec programó algo realmente inseguro, pero no podía renunciar a esa forma de hacer las cosas así como así, porque en realidad, parecía tratarse de una funcionalidad. Quizás por eso necesitó año y medio para solucionarlo. Al menos, aunque la vulnerabilidad era crítica, el componente vulnerable no se instalaba por defecto.

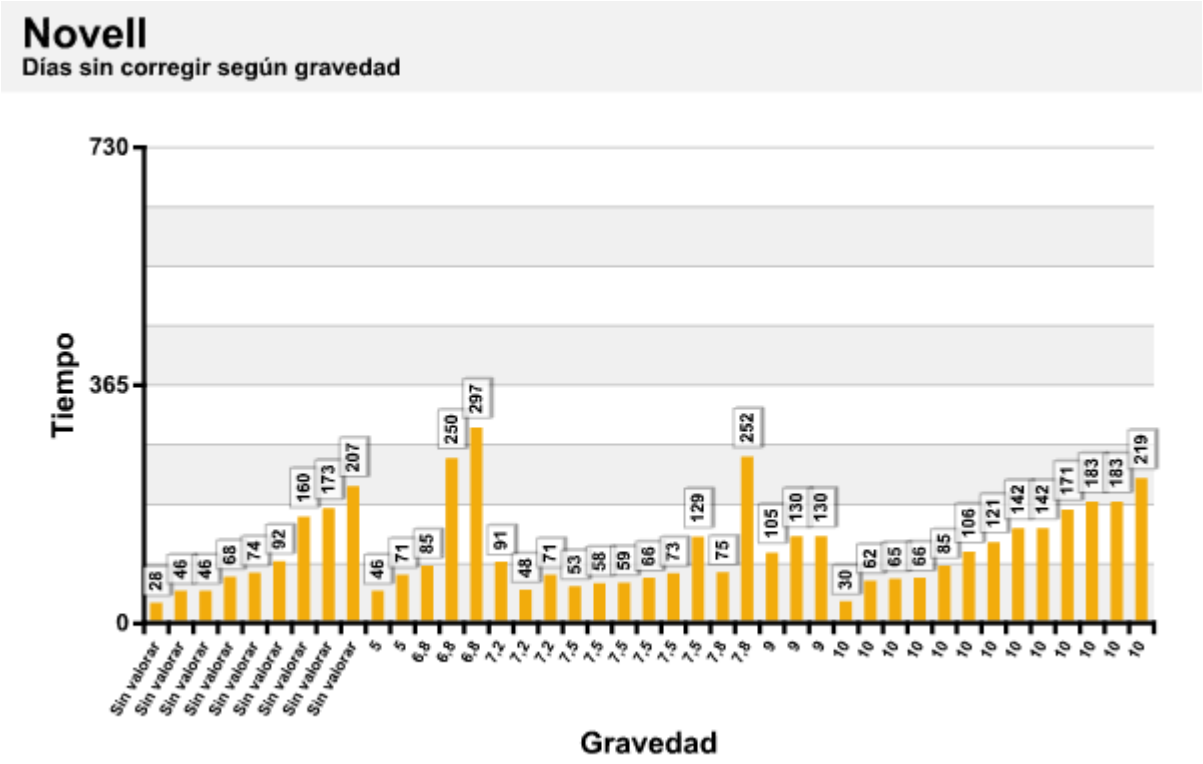
41 vulnerabilidades estudiadas.

Novell
Alertas según el número de días en resolver



Novell
Porcentaje de resolución según tiempo





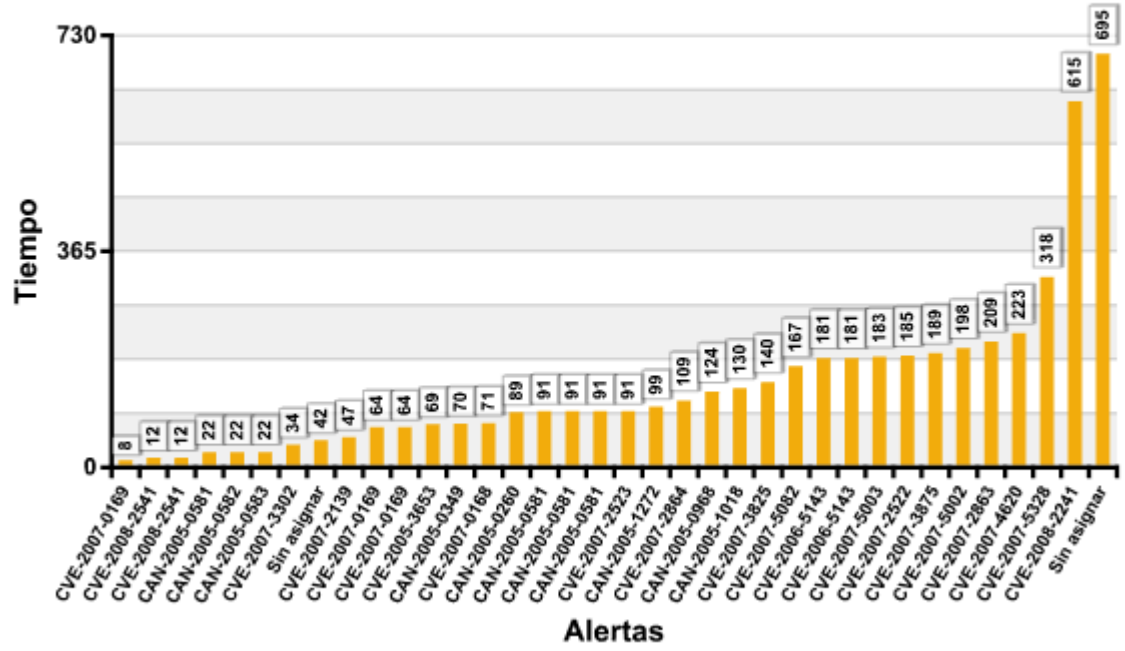
_ Curiosidades:

Novell sin duda es la que se muestra más regular. Esto se demuestra tanto “a simple vista” en la gráfica, como por su coeficiente de variación, el más bajo de todos los estudiados. Lo que significa que sus valores son los más regulares.

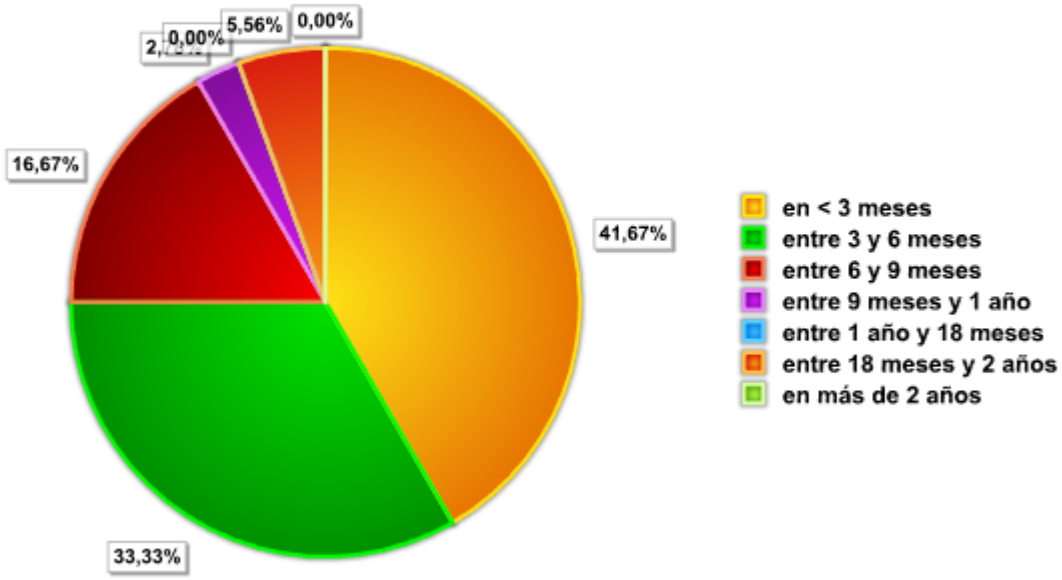
Computer Associates

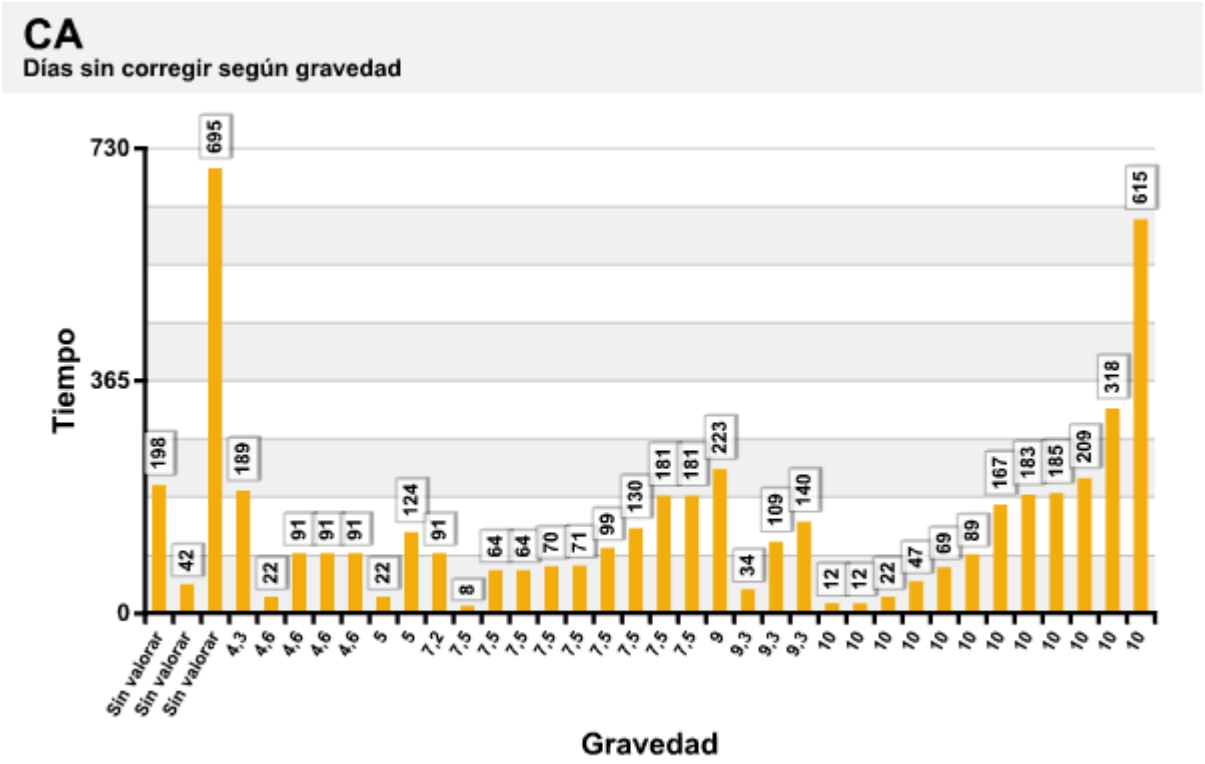
36 vulnerabilidades estudiadas.

CA
Alertas según el número de días en resolver



CA
Porcentaje de resolución según tiempo





_ Curiosidades:

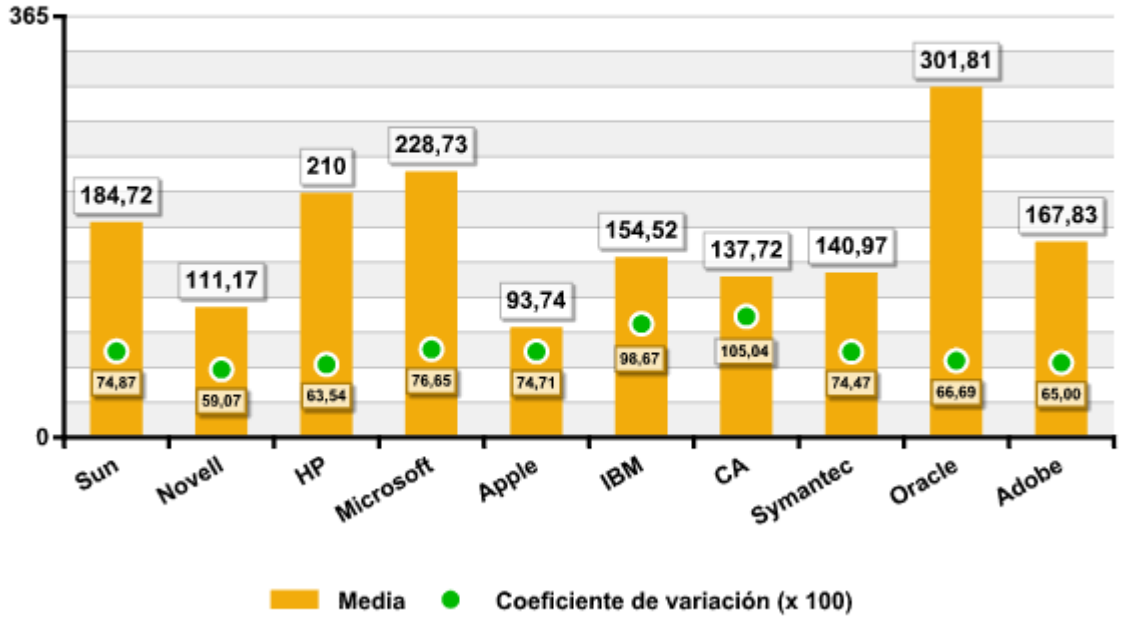
El ejemplo contrario a Novell, CA se muestra como bastante irregular, pudiendo tardar desde una semana a dos años en arreglar un problema de seguridad. Existen dos vulnerabilidades que claramente sobresalen por encima del resto, sin razón aparente justificada. Una de ellas, la CVE-2008-2241, permitía añadir datos a los ficheros existentes de logs en uno de sus productos más conocidos, el ARCserve Backup. Con poco esfuerzo, un atacante podía añadir datos al fichero de configuración y terminar así ejecutando código arbitrario. A pesar de la gravedad, CA le llevó más de año y medio solucionarlo. Aun así, cabe destacar que solo dos de sus vulnerabilidades han tardado más de un año en ser solucionadas.

Todos los fabricantes

449 vulnerabilidades estudiadas

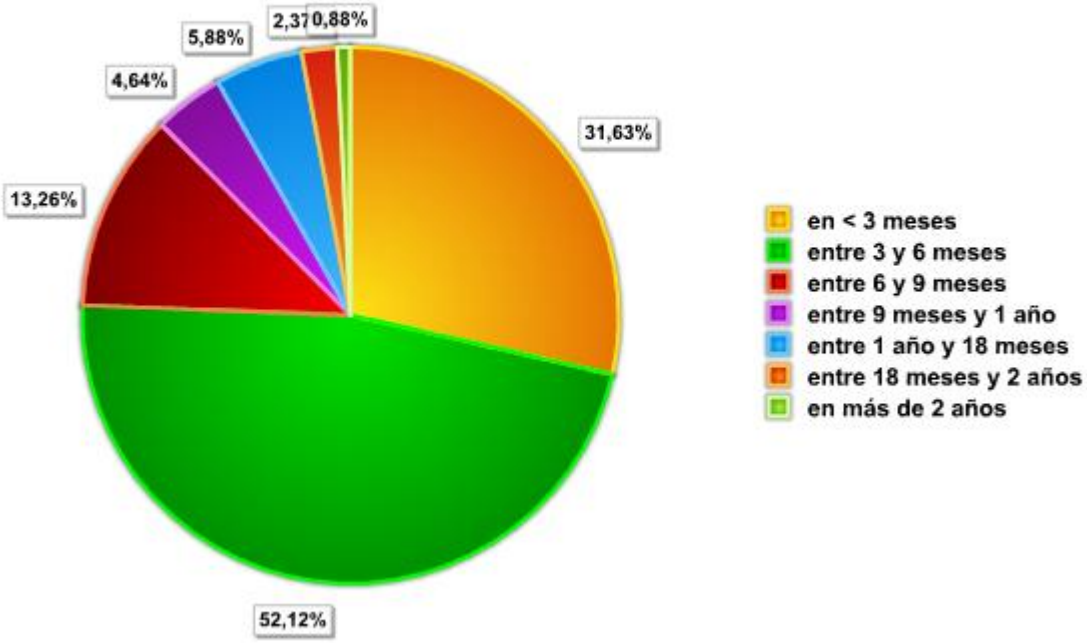
Media de días según fabricante

Un coeficiente de variación mayor indica que los valores que forman la media son más dispersos



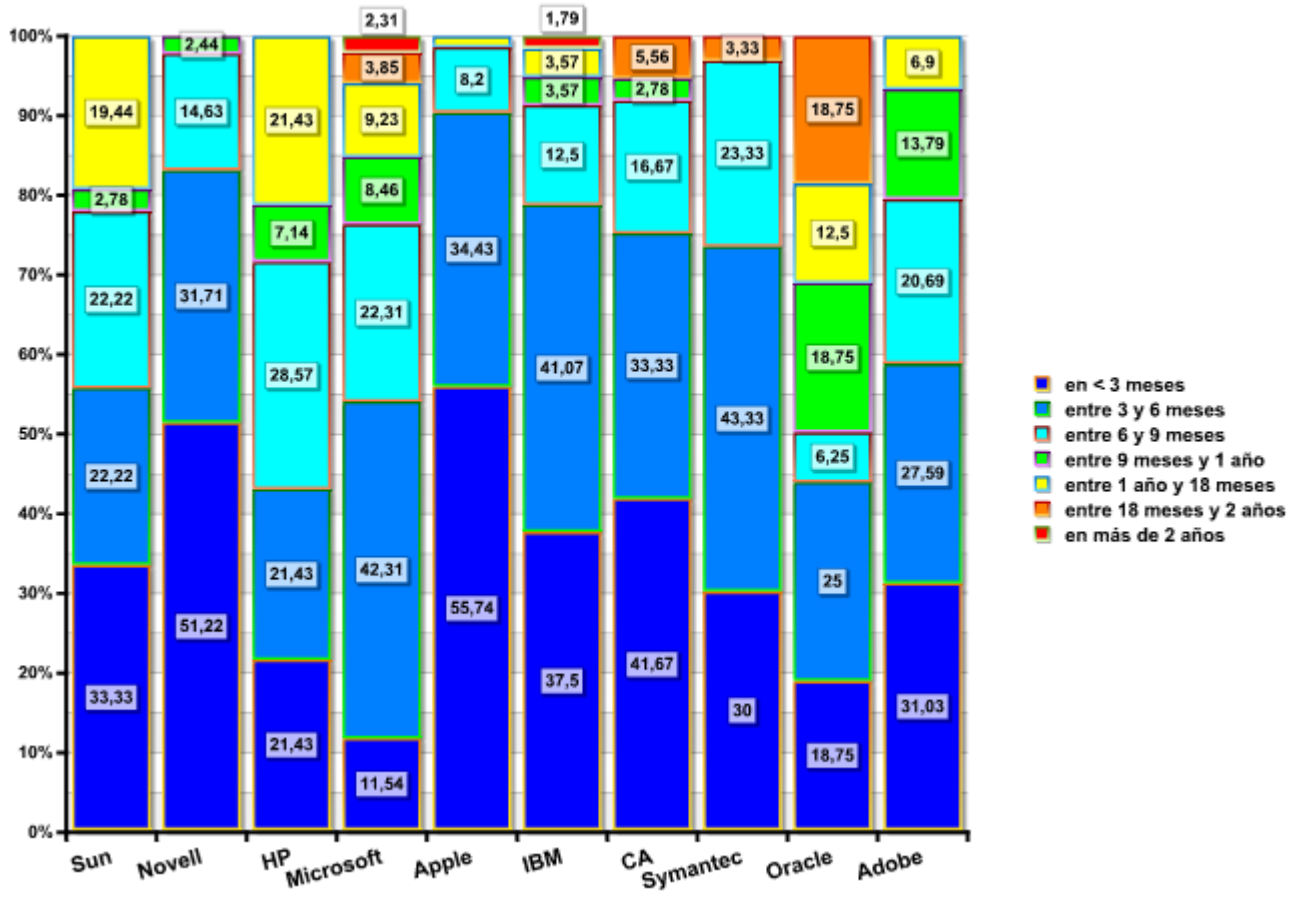
Todas las vulnerabilidades

Porcentaje de resolución según tiempo



Porcentaje de resolución de vulnerabilidades según tiempo

Comparación de porcentaje de resolución según tramos de tiempo



_ Conclusiones:

Se observa cómo el tiempo en general es abultado entre todos los fabricantes estudiados. Acumulan una media de 171,8 días, lo que **son casi 6 meses por vulnerabilidad**. De hecho, casi el 84% de las vulnerabilidades se resuelven antes de los 6 meses, y apenas un 10% pasa del año.

Se podrían clasificar en tres grandes grupos: Oracle, Microsoft y en menor medida HP como los más "perezosos" a la hora de solucionar vulnerabilidades no hechas públicas, con una media de entre 200 y 300 días (entre 7 y 10 meses). Por otro lado Apple y Novell se mantienen rondando los 100 días (más de 3 meses) para solucionar problemas de seguridad reportados de forma privada. El resto de fabricantes se mantienen entre los 3 y los 7 meses de media. Aunque Sun es uno de los fabricantes que más vulnerabilidades ha resuelto entre el año y los 18 meses. Lo que también cabe destacar son las vulnerabilidades puntuales que, por parte de casi todos los fabricantes, son resueltas bien en una semana, bien en año y medio o dos años, y que se salen totalmente de la media. Estos casos puntuales a veces tienen explicación y en ocasiones parecen no estar justificados.

Hispasec Sistemas

www.hispasec.com
info@hispasec.com
Telf: (+34) 902 161 025
Fax: (+34) 952 02 86 94

“Top Ten”

_ Las 10 vulnerabilidades más graves que más tiempo ha llevado resolver.

Fabric.	Vulnerabilidad	CVE	Grv	Día rep.	Día púb.	Días
Oracle	Oracle Secure Backup Administration Server login.php Command Injection Vulnerability	CVE-2008-5449	10	08/03/07	13/01/09	**677**
CA	CA BrightStor ARCserve Backup caloggerd Arbitrary File Writing Vulnerability	CVE-2008-2241	10	12/09/06	19/05/08	**615**
Oracle	Oracle Secure Backup exec_qr() Command Injection Vulnerability	CVE-2008-5448	10	13/07/07	14/01/09	**551**
IBM	IBM Tivoli Storage Manager Express Heap Buffer Overflow Vulnerability	CVE-2008-4563	10	22/07/08	03/10/09	**438**
Sun	Sun Java System Active Server Pages Buffer Overflow Vulnerability	CVE-2008-2404	10	04/04/07	03/06/08	**426**
Sun	Sun Java System Active Server Pages Multiple Directory Traversal Vulnerabilities	CVE-2008-2403	10	04/04/07	03/06/08	**426**
HP	HP OpenView Network Node Manager Multiple CGI Buffer Overflow	CVE-2007-6204	10	10/10/06	06/12/07	**422**
HP	HP Network Node Manager rping Stack Buffer Overflow Vulnerability	CVE-2009-1420	10	19/05/08	26/06/09	**403**
Adobe	Adobe Flash Media Server 2 Multiple Integer Overflow Vulnerabilities	CVE-2007-6149	10	27/11/07	02/12/08	**381**
HP	HP StorageWorks Storage Mirroring Authentication Processing Stack Overflow Vulnerability	CVE-2008-1661	10	22/05/07	04/06/08	**379**

_ Curiosidades:

HP es el fabricante que más veces aparece en esta lista, lo que significa que tarda más en resolver vulnerabilidades de criticidad maxima. Sun y Oracle le siguen de cerca.

“Top Ten”

_ Las 10 vulnerabilidades más rápidas en ser solucionadas.

Fabric.	Vulnerabilidad	CVE	Grv	Día rep.	Día púb.	Días
Apple	Apple QTJava toQTPointer() Pointer Arithmetic Memory Overwrite Vulnerability	CVE-2007-2175	7,6	23/04/07	01/05/07	8
CA	Computer Associates BrightStor ARCserve Backup RPC Engine PFC Request Buffer Overflow	CVE-2007-0169	7,5	03/01/07	11/01/07	8
Apple	Apple Mac OS X vpnd Server_id Buffer Overflow	CAN-2005-1343	7,2	25/04/05	04/05/05	9
CA	CA ETrust Secure Content Manager Gateway FTP PASV Stack Overflow Vulnerability	CVE-2008-2541	10	23/05/08	04/06/08	12
CA	CA ETrust Secure Content Manager Gateway FTP LIST Stack Overflow Vulnerability	CVE-2008-2541	10	23/05/08	04/06/08	12
Apple	Apple Mac OS X mDNSResponder HTTP Request Heap Overflow	CVE-2007-3744	5,8	26/07/07	07/08/07	12
HP	Hewlett-Packard HP-UX SLSd Arbitrary File Creation Vulnerability	CVE-0000-0000	X	30/01/07	13/02/07	14
Symantec	Symantec AntiVirus IOCTL Kernel Privilege Escalation	CVE-2006-4927	4,6	19/09/06	05/10/06	16
Adobe	Adobe Macromedia ColdFusion MX7 Insecure File Permissions	CVE-2007-1874	7,2	21/03/07	10/04/07	20
Apple	Apple Safari WebKit PCRE Handling Integer Overflow Vulnerability	CVE-2008-1026	6,8	27/03/08	16/04/08	20

_ Curiosidades:

Apple y CA son las más rápidas en resolver varias de estas vulnerabilidades. CA, incluso, cuando la gravedad de estas (10 sobre 10) así lo requerían.

“Top Ten”

_ Las 10 vulnerabilidades que más han tardado en ser solucionadas.

Fabric.	Vulnerabilidad	CVE	Grv	Día rep.	Día púb.	Días
IBM	IBM AIX swcons Local Arbitrary File Acces	CVE-0000-0000	X	21/12/04	30/10/07	1043
Microsoft	Microsoft Word 2000 WordPerfect 6.x Converter Stack Corruption Vulnerability	CVE-2009-0088	9,3	28/06/06	14/04/09	1021
Microsoft	Microsoft Office OWC10.Spreadsheet ActiveX msDataSourceObject() Heap Corruption Vulnerability	CVE-2009-1136	9,3	19/03/07	11/08/09	876
Microsoft	Microsoft Office OWC10 ActiveX Control Loading and Unloading Heap Corruption Vulnerability	CVE-2009-0562	9,3	29/03/07	11/08/09	866
Microsoft	Microsoft Office BMP Input Filter Heap Overflow	CVE-0000-0000	X	11/09/06	12/08/08	701
Microsoft	Microsoft Windows Graphics Rendering Engine PICT Heap Corruption	CVE-2008-3021	9,3	14/09/06	12/08/08	698
CA	CA Unicenter Software Delivery dtscore.dll Stack Overflow Vulnerability	CVE-0000-0000	X	14/09/07	07/08/09	695
Oracle	Oracle E-Business Suite Business Intelligence SQL Injection Vulnerability	CVE-0000-0000	X	29/01/07	16/12/08	687
Oracle	Oracle Secure Backup Administration Server login.php Command Injection Vulnerability	CVE-2008-5449	10	08/03/07	13/01/09	677
Microsoft	Microsoft Office WPG Image File Heap Buffer Overflow	CVE-2008-3460	9,3	07/11/06	12/08/08	644

_ Curiosidades:

Microsoft, aunque su media no sea la mayor de todos los fabricantes, sí que ha situado varias vulnerabilidades como las más duraderas, incluso resultando realmente graves (9,3 sobre 10). 6 vulnerabilidades de este “top ten” de las vulnerabilidades más persistentes, son suyas.

Anexo

_ Detalle de todas las vulnerabilidades estudiadas:

Fabricante	Vulnerabilidad	CVE	Grav.	Día rep.	Día púb.	Días
Sun	Sun Java Runtine Environment (JRE) Type1 Font Parsing Integer Signedness Vulnerability	CVE-0000-0000	X	18/02/09	25/03/09	35
Sun	Sun Microsystems Solaris FIFO FS Information Disclosure Vulnerability	CVE-0000-0000	X	13/02/07	02/10/07	231
Sun	Sun Java JRE TrueType Font Parsing Heap Overflow Vulnerability	CVE-0000-0000	X	10/09/08	02/12/08	83
Sun	Sun Java JRE TrueType Font Parsing Integer Overflow Vulnerability	CVE-0000-0000	X	31/07/08	02/12/08	124
Sun	Sun Java Web Proxy Server FTP Resource Handling Heap-Based Buffer Overflow	CVE-2008-4541	10	27/05/08	09/10/08	135
Sun	Sun Solaris snoop SMB Decoding Multiple Stack Buffer Overflow Vulnerabilities	CVE-2008-0964	9,3	23/01/08	04/08/08	193
Sun	Sun Java AWT Library Sandbox Violation Vulnerability	CVE-2008-5359	9,3	16/04/08	04/12/08	232
Sun	Sun Java System Active Server Pages File Creation Vulnerability	CVE-2008-2401	7,5	04/04/07	03/06/08	426
Sun	Sun Microsystems Solaris srsexec Format String Vulnerability	CVE-2007-3880	7,2	18/07/07	02/11/07	107
Sun	Sun Microsystems Java GIF File Parsing Memory Corruption Vulnerability	CVE-2007-0243	6,8	16/06/06	16/01/07	214
Sun	Sun Java Web Start (JWS) GIF Decoding Heap Corruption	CVE-0000-0000	X	18/02/09	25/03/09	35
Sun	Sun Java Runtine Environment (JRE) GIF Decoding Heap Corruption	CVE-0000-0000	X	18/02/09	25/03/09	35
Sun	Sun Java Web Start (JWS) PNG Decoding Integer Overflow	CVE-0000-0000	X	18/02/09	25/03/09	35
Sun	Sun Java Runtime Environment (JRE) Pack200 Decompression Integer Overflow	CVE-0000-0000	X	09/01/09	25/03/09	75
Sun	Sun Java Web Start GIF Decoding Memory Corruption	CVE-0000-0000	X	01/10/08	02/12/08	62
Sun	Sun Java JRE Pack200 Decompression Integer Overflow	CVE-0000-0000	X	02/10/08	02/12/08	61
Sun	Sun Java System Active Server Pages Information Disclosure	CVE-2008-2402	5	04/04/07	03/06/08	426
Sun	Sun Java System Active Server Pages Multiple Directory Traversal Vulnerabilities	CVE-2008-2403	10	04/04/07	03/06/08	426
Sun	Sun Java System Active Server Pages Buffer Overflow Vulnerability	CVE-2008-2404	10	04/04/07	03/06/08	426
Sun	Sun Java System Active Server Pages Multiple Command Injection	CVE-2008-2405	7,5	11/05/07	03/06/08	389
Sun	Sun Java System Active Server Pages Authorization Bypass Vulnerability	CVE-2008-2406	7,5	11/05/07	03/06/08	389
Sun	Sun Java System Web Proxy Multiple Buffer Overflow	CVE-0000-0000	X	20/03/07	25/05/07	66

Sun	Sun Microsystems Solaris SRS Proxy Core srsexec Arbitrary File Read	CVE-0000-0000	X	07/11/06	10/05/07	184
Sun	Sun Microsystems Solaris ACE_SETACL Integer Signedness DoS Vulnerability	CVE-0000-0000	X	07/11/06	07/05/07	181
Sun	Sun Java System Directory Server 5.2 Uninitialized Pointer Cleanup Design Error Vulnerability	CVE-2006-4175	7,8	16/08/06	23/03/07	219
Sun	Sun Microsystems Solaris ld.so Directory Traversal	CVE-0000-0000	X	24/10/06	12/12/06	49
Sun	Sun Microsystems Solaris ld.so 'doprf()' Buffer Overflow	CVE-0000-0000	X	24/10/06	12/12/06	49
Sun	Sun Microsystems Solaris NSPR Library Arbitrary File Creation	CVE-0000-0000	X	31/08/06	11/10/06	41
Sun	Sun Microsystems Solaris sysinfo() Kernel Memory Disclosure	CVE-0000-0000	X	15/12/05	20/07/06	217
Sun	Sun Solaris uustat Buffer Overflow Vulnerability	CVE-0000-0000	X	11/08/04	10/01/06	517
Sun	Sun Solaris kcms_configure Arbitrary File Corruption	CVE-0000-0000	X	27/04/04	23/02/05	302
Sun	Sun Java Web Start and Applet Multiple Sandbox Bypass Vulnerabilities	CVE-2008-5339	5	14/07/08	04/12/08	143
Sun	Sun Java Web Start vm args Stack-Based Buffer Overflow Vulnerability	CVE-2008-3111	10	17/01/08	17/07/08	182
Sun	Sun Java Runtime Environment (JRE) Pack200 Decompression Integer Overflow Vulnerability	CVE-0000-0000	X	09/04/09	04/08/09	117
Sun	Sun Java Pack200 Decoding Inner Class Count Integer Overflow Vulnerability	CVE-0000-0000	X	15/04/09	05/08/09	112
Sun	Sun Java Web Start JPEG Header Parsing Integer Overflow Vulnerability	CVE-0000-0000	X	26/03/09	05/08/09	132
HP	HP Network Node Manager rping Stack Buffer Overflow Vulnerability	CVE-2009-1420	10	19/05/08	26/06/09	403
HP	HP Network Node Manager Multiple Command Injection Vulnerabilities	CVE-2008-4559	10	19/06/08	06/02/09	232
HP	HP Network Node Manager Multiple Information Disclosure Vulnerabilities	CVE-2008-4560	7,8	19/06/08	06/02/09	232
HP	Hewlett-Packard Mercury Quality Center ActiveX Control ProgColor Buffer Overflow Vulnerability	CVE-0000-0000	X	16/02/07	02/04/07	45
HP	Hewlett-Packard OVIS Probe Builder Arbitrary Process Termination Vulnerability	CVE-2008-1667	7,8	03/04/08	28/07/08	116
HP	Hewlett-Packard Network Node Manager Topology Manager Service DoS Vulnerability	CVE-2008-0212	7,8	14/05/07	04/02/08	266
HP	Hewlett-Packard OpenView Operations OVTrace Buffer Overflow Vulnerabilities	CVE-2007-3872	6,8	12/07/07	09/08/07	28
HP	Hewlett-Packard HP-UX SLSd Arbitrary File Creation Vulnerability	CVE-0000-0000	X	30/01/07	13/02/07	14
HP	HP StorageWorks Storage Mirroring Authentication Processing Stack Overflow Vulnerability	CVE-2008-1661	10	22/05/07	04/06/08	379
HP	Hewlett-Packard HP-UX swagentd Buffer Overflow Vulnerability	CVE-2007-6195	7,8	20/07/07	17/12/07	150

HP	HP Network Node Manager ovlaunch CGI BSS Overflow Vulnerability	CVE-2008-4562	10	19/06/08	06/02/09	232
HP	HP OpenView Network Node Manager Multiple CGI Buffer Overflow	CVE-2007-6204	10	10/10/06	06/12/07	422
HP	HP OpenView Radia Integration Server File System Exposure	CVE-2007-5413	7,8	18/12/06	31/10/07	317
HP	HP Mercury LoadRunner Agent Stack Overflow	CVE-2007-0446	10	27/10/06	08/02/07	104
Novell	Novell NetMail IMAPD Command Continuation Request Heap Overflow	CAN-2005-1758	7,5	25/04/05	01/09/05	129
Novell	Novell NetMail IMAPD subscribe Buffer Overflow Vulnerability	CVE-0000-0000	X	10/10/06	23/12/06	74
Novell	Novell Netmail IMAP append Denial of Service Vulnerability	CVE-0000-0000	X	16/10/06	23/12/06	68
Novell	Novell ZENworks Asset Management Collection Client Heap Overflow Vulnerability	CVE-0000-0000	X	16/10/06	01/12/06	46
Novell	Novell ZENworks Asset Management Msg.dll Heap Overflow Vulnerability	CVE-0000-0000	X	16/10/06	01/12/06	46
Novell	Novell iManager Tomcat DoS Vulnerability	CVE-2006-4517	7,8	17/08/06	31/10/06	75
Novell	Novell eDirectory NMAS BerDecodeLoginDataRequeset DoS Vulnerability	CVE-2006-4521	5	17/08/06	27/10/06	71
Novell	Novell eDirectory NCP over IP length Heap Overflow	CVE-2006-4177	7,5	16/08/06	21/10/06	66
Novell	Novell eDirectory evtFilteredMonitorEventsRequest Heap Overflow	CVE-2006-4509	10	16/08/06	21/10/06	66
Novell	Novell eDirectory evtFilteredMonitorEventsRequest Invalid Free	CVE-2006-4510	10	16/08/06	21/10/06	65
Novell	Novell GroupWise Messenger nmma.exe DoS Vulnerability	CVE-2006-4511	5	17/08/06	02/10/06	46
Novell	Novell SUSE Linux Enterprise Server Remote Manager Heap Overflow	CVE-2005-3655	7,5	15/11/05	13/01/06	59
Novell	Novell ZENworks Endpoint Security Management Local Privilege Escalation	CVE-2007-5665	7,2	24/09/07	24/12/07	91
Novell	Novell NetWare Client NWFILTER.SYS Local Privilege Escalation Vulnerability	CVE-2007-5667	7,2	25/09/07	12/11/07	48
Novell	Novell NetMail NMDMC Buffer Overflow Vulnerability	CVE-0000-0000	X	07/02/07	10/05/07	92
Novell	Novell eDirectory NCP Fragment Denial of Service Vulnerability	CVE-2006-4520	7,8	17/08/06	26/04/07	252
Novell	Novell eDirectory NCP Get Extension Information Request Memory Corruption	CVE-0000-0000	X	10/03/08	03/10/08	207
Novell	Novell eDirectory LDAP Search Request Heap Corruption Vulnerability	CVE-2008-1809	10	10/03/08	09/07/08	121
Novell	Novell NetWare Client nicm.sys Local Privilege Escalation Vulnerability	CVE-2007-5762	7,2	30/10/07	09/01/08	71
Novell	Novell Privileged User Manager Remote DLL Injection Vulnerability	CVE-0000-0000	X	23/06/09	21/07/09	28
Novell	Novell Client/NetIdentity Agent Remote Arbitrary Pointer Dereference Code Execution	CVE-0000-0000	X	15/10/08	06/04/09	173

	Vulnerability					
Novell	Novell Netware Groupwise GWIA RCPT Command Buffer Overflow Vulnerability	CVE-0000-0000	X	26/08/08	02/02/09	160
Novell	Novell eDirectory Core Protocol Opcode 0x24 Heap Overflow Vulnerability	CVE-2008-4480	10	19/05/08	08/10/08	142
Novell	Novell eDirectory Core Protocol Opcode 0x0F Heap Overflow Vulnerability	CVE-2008-4478	10	19/05/08	08/10/08	142
Novell	Novell eDirectory dhost.exe Accept Language Header Heap Overflow Vulnerability	CVE-2008-4479	10	08/04/08	08/10/08	183
Novell	Novell eDirectory dhost.exe Content-Length Header Heap Overflow Vulnerability	CVE-2008-4478	10	08/04/08	08/10/08	183
Novell	Novell eDirectory dhost Integer Overflow Code Execution Vulnerability	CVE-2008-3159	10	04/12/07	10/07/08	219
Novell	Novell eDirectory for Linux LDAP delRequest Stack Overflow Vulnerability	CVE-2008-0924	6,8	20/07/07	26/03/08	250
Novell	Novell Client NWSPOOL.DLL EnumPrinters Stack Overflow Vulnerability	CVE-2008-0639	10	11/12/07	11/02/08	62
Novell	Novell NetMail AntiVirus Agent Multiple Heap Overflow Vulnerabilities	CVE-2007-6302	6,8	16/02/07	10/12/07	297
Novell	Novell Client Trust Heap Overflow Vulnerability	CVE-2007-5767	10	17/07/07	31/10/07	106
Novell	Novell Client NWSPOOL.DLL Stack Overflow Vulnerability	CVE-2007-2954	10	16/02/07	06/08/07	171
Novell	Novell Groupwise WebAccess Base64 Decoding Stack Overflow Vulnerability	CVE-2007-2171	10	19/03/07	18/04/07	30
Novell	Novell Netmail WebAdmin Buffer Overflow Vulnerability	CVE-2007-1350	6,8	12/12/06	07/03/07	85
Novell	Novell NetMail IMAP APPEND Buffer Overflow Vulnerability	CVE-2006-6425	9	14/08/06	22/12/06	130
Novell	Novell NetMail IMAP Verb Literal Heap Overflow Vulnerability	CVE-2006-6424	9	14/08/06	22/12/06	130
Novell	Novell NetMail NMAP STOR Buffer Overflow Vulnerability	CVE-2006-6424	9	08/09/06	22/12/06	105
Novell	Novell Netware Client Print Provider Buffer Overflow Vulnerability	CVE-2006-5854	7,5	02/10/06	29/11/06	58
Novell	Novell Netmail User Authentication Buffer Overflow Vulnerability	CVE-2006-5478	7,5	08/09/06	31/10/06	53
Novell	Novell eDirectory NDS Server Host Header Buffer Overflow Vulnerability	CVE-2006-5478	7,5	14/08/06	26/10/06	73
Novell	Novell eDirectory 8.8 NDS Server Buffer Overflow Vulnerability	CVE-2006-2496	10	20/03/06	13/06/06	85
Microsoft	Microsoft Embedded OpenType Font Engine (T2EMBED.DLL) Heap Buffer Overflow Vulnerability	CVE-2009-0231	9,3	25/08/08	14/07/09	323
Microsoft	Microsoft Office Publisher 2007 Arbitrary Pointer Dereference Vulnerability	CVE-2009-0566	9,3	08/01/09	14/07/09	187
Microsoft	Microsoft Active Directory Hexdecimal DN AttributeValue Invalid Free Vulnerability	CVE-2009-1138	10	21/01/09	11/06/09	141
Microsoft	Microsoft Excel SST Record Integer Overflow Vulnerability	CVE-2009-0561	9,3	19/02/09	09/06/09	110

Microsoft	Microsoft Windows 2000 Print Spooler Remote Stack Buffer Overflow Vulnerability	CVE-2009-0228	10	05/09/08	09/06/09	277
Microsoft	Microsoft PowerPoint 4.2 Conversion Filter Stack Buffer Overflow Vulnerability	CVE-2009-0227	9,3	03/12/08	12/05/09	160
Microsoft	Microsoft SQL Server Restore Integer Underflow Vulnerability	CVE-2008-0107	9	06/12/07	08/07/08	215
Microsoft	Microsoft Internet Explorer HTML Tag Long File Name Extension Stack Buffer Overflow Vulnerability	CVE-2008-4261	9,3	26/08/08	09/12/08	105
Microsoft	Microsoft Windows Graphics Device Interface Integer Overflow Vulnerability	CVE-2008-2249	9,3	21/05/08	09/12/08	202
Microsoft	Microsoft DirectShow Quicktime Atom Parsing Memory Corruption Vulnerability	CVE-2009-1539	9,3	23/09/08	14/07/09	294
Microsoft	Microsoft Internet Explorer 8 Rows Property Dangling Pointer Code Execution	CVE-2009-1532	9,3	19/03/09	10/06/09	83
Microsoft	Microsoft Office Excel QSIR Record Pointer Corruption	CVE-2009-1134	9,3	26/03/09	10/06/09	76
Microsoft	Microsoft Internet Explorer onreadystatechange Memory Corruption	CVE-2009-1531	9,3	26/01/09	10/06/09	135
Microsoft	Microsoft Internet Explorer Event Handler Memory Corruption	CVE-2009-1530	9,3	26/01/09	10/06/09	135
Microsoft	Microsoft Internet Explorer Concurrent Ajax Request Memory Corruption	CVE-2009-1528	9,3	15/01/09	10/06/09	144
Microsoft	Microsoft Internet Explorer setCapture Memory Corruption	CVE-2009-1529	9,3	26/01/09	10/06/09	135
Microsoft	Microsoft Word Document Stack Based Buffer Overflow	CVE-2009-0563	9,3	08/07/08	10/06/09	337
Microsoft	Microsoft Office PowerPoint OutlineTextRefAtom Parsing Memory Corruption	CVE-2009-0556	9,3	07/04/08	12/05/09	400
Microsoft	Microsoft Internet Explorer Malformed CSS Memory Corruption	CVE-2009-0076	9,3	15/10/08	10/02/09	118
Microsoft	Microsoft Internet Explorer CFunctionPointer Memory Corruption	CVE-2009-0075	8,5	23/09/08	10/02/09	140
Microsoft	Microsoft SMB NT Trans2 Request Parsing Remote Code Execution	CVE-2008-4835	10	14/08/08	13/01/09	152
Microsoft	Microsoft SMB NT Trans Request Parsing Remote Code Execution	CVE-2008-4834	10	25/06/08	13/01/09	202
Microsoft	Microsoft Internet Explorer Webdav Request Parsing Heap Corruption	CVE-2008-4259	9,3	19/05/08	09/12/08	204
Microsoft	Microsoft Office Word Document Table Property Stack Overflow	CVE-2008-4837	9,3	19/08/08	09/12/08	112
Microsoft	Microsoft Office RTF Drawing Object Heap Overflow	CVE-2008-4028	9,3	25/06/08	09/12/08	167
Microsoft	Microsoft Office RTF Consecutive Drawing Object Parsing Heap Corruption	CVE-2008-4027	9,3	19/05/08	09/12/08	204
Microsoft	Microsoft Animation ActiveX Control Malformed AVI Parsing Code Execution	CVE-2008-4255	8,5	16/09/08	09/12/08	84
Microsoft	Microsoft Internet Explorer componentFromPoint Memory Corruption	CVE-2008-3475	9,3	25/06/08	14/10/08	111
Microsoft	Microsoft Office Excel BIFF File Format Parsing Stack Overflow	CVE-2008-3471	9,3	23/05/08	14/10/08	144

Microsoft	Microsoft Windows GDI+ GIF Parsing Code Execution	CVE-2008-3013	9,3	07/02/08	09/09/08	215
Microsoft	Microsoft Windows GDI+ BMP Parsing Code Execution	CVE-2008-3015	9,3	20/07/07	09/09/08	417
Microsoft	Microsoft Internet Explorer Table Layout Memory Corruption	CVE-2008-2258	9,3	16/04/08	12/08/08	118
Microsoft	Microsoft Internet Explorer XHTML Rendering Memory Corruption	CVE-2008-2257	9,3	16/04/08	12/08/08	118
Microsoft	Microsoft Windows Graphics Rendering Engine PICT Heap Corruption	CVE-2008-3021	9,3	14/09/06	12/08/08	698
Microsoft	Microsoft Excel COUNTRY Record Memory Corruption	CVE-2008-3006	9,3	16/04/08	12/08/08	118
Microsoft	Microsoft DirectX SAMI File Format Name Parsing Stack Overflow	CVE-0000-0000	X	21/01/08	10/06/08	141
Microsoft	Microsoft Internet Explorer DOM Object substringData() Heap Overflow	CVE-2008-1442	9,3	07/02/08	10/06/08	124
Microsoft	Microsoft Office RTF Parsing Engine Memory Corrupti	CVE-2008-1091	9,3	21/01/08	13/05/08	113
Microsoft	Microsoft GDI WMF Parsing Heap Overflow	CVE-2008-1083	9,3	07/02/08	08/04/08	61
Microsoft	Microsoft Excel BIFF File Format Cell Record Parsing Memory Corruption	CVE-2008-0113	9,3	22/05/07	11/03/08	294
Microsoft	Microsoft Internet Explorer SVG animateMotion.by Code Execution	CVE-2008-0077	9,3	17/09/07	12/02/08	148
Microsoft	Microsoft Office Publisher 2007 Arbitrary Pointer Dereference	CVE-2009-0566	9,3	08/01/09	14/07/09	187
Microsoft	Microsoft Excel SST Record Integer Overflow	CVE-2009-0561	9,3	19/02/09	09/06/09	110
Microsoft	Microsoft PowerPoint 4.2 Conversion Filter Stack Buffer Overflow	CVE-2009-0227	9,3	03/12/08	12/05/09	160
Microsoft	Microsoft PowerPoint 4.2 Conversion Filter Heap Corruption Vulnerability	CVE-2009-0223	9,3	24/02/09	12/05/09	77
Microsoft	Microsoft PowerPoint 4.2 Conversion Filter Stack Overflow	CVE-2009-0226	9,3	03/12/08	12/05/09	160
Microsoft	Microsoft PowerPoint PPT 4.0 Importer Multiple Stack Buffer Overflow	CVE-2009-0220	9,3	29/08/08	12/05/09	256
Microsoft	Microsoft PowerPoint PPT95 Import Multiple Stack Buffer Overflow	CVE-2009-1129	9,3	25/04/08	12/05/09	382
Microsoft	Microsoft PowerPoint PPT95 Import Multiple Stack Buffer Overflow	CVE-2009-1128	9,3	16/06/08	12/05/09	330
Microsoft	Microsoft PowerPoint Build List Memory Corruption	CVE-2009-0224	9,3	06/10/08	12/05/09	218
Microsoft	Microsoft PowerPoint Notes Container Heap Corruption	CVE-2009-1130	9,3	22/10/08	12/05/09	202
Microsoft	Microsoft PowerPoint Integer Overflow	CVE-2009-0221	9,3	03/09/08	12/05/09	251
Microsoft	Microsoft WordPad Word97 Converter Stack Buffer Overflow	CVE-2009-0235	9,3	19/12/08	14/04/09	116
Microsoft	Microsoft Excel Malformed Object Memory Corruption Vulnerability	CVE-2008-4265	9,3	21/07/08	09/12/08	141

Microsoft	Microsoft Host Integration Server 2006 Command Execution	CVE-2008-3466	10	27/05/08	14/10/08	140
Microsoft	Microsoft Visual Basic for Applications - Multiple Vulnerabilities	CVE-2008-3477	9,3	17/04/07	14/10/08	546
Microsoft	Microsoft Windows GDI+ Gradient Fill Heap Overflow	CVE-2007-5348	9,3	09/05/07	09/09/08	489
Microsoft	Microsoft Office BMP Input Filter Heap Overflow	CVE-0000-0000	X	11/09/06	12/08/08	701
Microsoft	Microsoft Office WPG Image File Heap Buffer Overflow	CVE-2008-3460	9,3	07/11/06	12/08/08	644
Microsoft	Microsoft PowerPoint Viewer 2003 Out of Bounds Array Index	CVE-2008-0121	9,3	28/09/07	12/08/08	319
Microsoft	Microsoft PowerPoint Viewer 2003 Cstring Integer Overflow	CVE-2008-0120	9,3	28/09/07	12/08/08	319
Microsoft	Microsoft Excel Chart AxesSet Invalid Array Index	CVE-2008-3004	9,3	27/03/08	12/08/08	138
Microsoft	Microsoft Excel FORMAT Record Invalid Array Index	CVE-2008-3005	9,3	27/03/08	12/08/08	138
Microsoft	Microsoft Windows Color Management Module Heap Buffer Overflow	CVE-0000-0000	X	10/04/08	12/08/08	124
Microsoft	Microsoft Word CSS Processing Memory Corruption	CVE-2008-1434	9,3	08/11/07	13/05/08	187
Microsoft	Microsoft Windows I2O Filter Utility Driver (i2omgmt.sys) Local Privilege Escalation	CVE-2008-0322	7,2	20/03/07	12/05/08	419
Microsoft	Microsoft HxTocCtrl ActiveX Control Invalid Param Heap Corruption	CVE-2008-1086	9,3	12/12/06	08/04/08	483
Microsoft	Microsoft Windows Graphics Rendering Engine Integer Overflow	CVE-0000-0000	X	17/12/07	08/04/08	113
Microsoft	Microsoft Windows Graphics Rendering Engine Heap Buffer Overflow	CVE-2008-1083	9,3	17/12/07	08/04/08	113
Microsoft	Microsoft Excel DVAL Heap Corruption	CVE-2008-0111	9,3	09/05/07	11/03/08	307
Microsoft	Microsoft Excel 2003 Malformed Formula Memory Corruption	CVE-0000-0000	X	27/07/07	11/03/08	228
Microsoft	Microsoft Outlook mailto Command Line Switch Injection	CVE-2008-0110	9,3	03/07/07	11/03/08	252
Microsoft	Microsoft Office Works Converter Heap Overflow Vulnerability	CVE-2007-0216	9,3	13/11/06	12/02/08	456
Microsoft	Microsoft Office Works Converter Stack-based Buffer Overflow	CVE-2008-0108	9,3	14/06/07	12/02/08	243
Microsoft	Microsoft Internet Explorer Property Memory Corruption	CVE-2008-0077	9,3	24/10/07	12/02/08	111
Microsoft	Microsoft Internet Explorer JavaScript setExpression Heap Corruption	CVE-2007-3902	9,3	08/05/07	11/12/07	217
Microsoft	Microsoft DirectX 7 and 8 DirectShow Stack Buffer Overflow	CVE-2007-3901	8,5	28/09/07	11/12/07	74
Microsoft	Microsoft DebugView Privilege Escalation	CVE-2007-4223	10	21/08/07	06/11/07	77
Microsoft	Microsoft Windows Mail and Outlook Express NNTP Protocol Heap	CVE-2007-3897	9,3	11/07/07	09/10/07	90

Microsoft	Microsoft Windows 2000 Agent URL Canonicalizing Stack Based Buffer Overflow	CVE-2007-3040	9,3	09/07/07	11/09/07	64
Microsoft	Microsoft Windows Vista Sidebar RSS Feeds Gadget Cross Site Scripting	CVE-2007-3033	6,8	21/03/07	14/08/07	146
Microsoft	Microsoft XML Core Services XMLDOM Memory Corruption	CVE-2007-2223	9,3	17/05/06	14/08/07	454
Microsoft	Microsoft DirectX RLE Compressed Targa Image File Heap Overflow	CVE-2006-4183	6,8	16/08/06	18/07/07	336
Microsoft	Microsoft License Manager and urlmon.dll COM Object Interaction Invalid Memory Access	CVE-2007-0218	9,3	24/10/06	12/06/07	231
Microsoft	Microsoft Word RTF File Parsing Heap Corruption	CVE-0000-0000	X	27/02/07	08/05/07	70
Microsoft	Microsoft Exchange Server 2000 IMAP Literal Processing Do	CVE-2007-0221	7,8	10/01/07	08/05/07	118
Microsoft	Microsoft Excel Filter Record Code Execution	CVE-2007-1214	6,8	08/02/07	08/05/07	89
Microsoft	Microsoft Windows Universal Plug and Play Memory Corruptio	CVE-2007-1204	6,8	06/12/06	10/04/07	125
Microsoft	Microsoft Windows WMF Triggerable Kernel Design Error DoS	CVE-2007-1211	7,1	10/01/06	03/04/07	448
Microsoft	Microsoft 'wininet.dll' FTP Reply Null Termination Heap Corruption	CVE-2007-0217	10	16/08/06	13/02/07	181
Microsoft	Microsoft Excel Invalid Column Heap Corruption	CVE-2007-0030	9,3	14/09/06	09/01/07	117
Microsoft	Microsoft Excel Long Palette Heap Overflow	CVE-2007-0031	9,3	22/09/06	09/01/07	109
Microsoft	Microsoft Windows VML Element Integer Overflow	CVE-2007-0024	9,3	03/10/06	09/01/07	98
Microsoft	Microsoft Windows Media Player Plugin Buffer Overflow	CVE-2006-0005	9,3	31/08/05	14/02/06	167
Microsoft	Microsoft Distributed Transaction Controller Packet Relay DoS Vulnerability	CAN-2005-1980	5	23/03/05	11/10/05	202
Microsoft	Microsoft Distributed Transaction Controller TIP DoS Vulnerability	CAN-2005-1979	5	23/03/05	11/10/05	202
Microsoft	Microsoft Word 2000 and Word 2002 Font Parsing Buffer Overflow	CAN-2005-0564	7,5	24/03/05	12/07/05	110
Microsoft	Microsoft Outlook Web Access Cross-Site Scripting	CAN-2005-0563	4,3	08/04/05	14/06/05	67
Microsoft	Microsoft Windows Interactive Training Buffer Overflow	CAN-2005-1212	7,5	23/02/05	14/06/05	111
Microsoft	Microsoft Outlook Express NNTP Response Parsing Buffer Overflow	CAN-2005-1213	7,5	16/11/04	14/06/05	210
Microsoft	Microsoft Internet Explorer DHTML Engine Race Condition Vulnerability	CAN-2005-0553	5,1	25/10/04	12/04/05	169
Microsoft	Microsoft Windows Internet Explorer Long Hostname Heap Corruption	CAN-2005-0554	7,5	11/11/04	12/04/05	152
Microsoft	Microsoft Windows CSRSS.EXE Stack Overflow	CAN-2005-0551	10	04/01/05	12/04/05	98
Microsoft	Microsoft MSHTA Script Execution	CVE-0000-0000	X	02/11/04	12/04/05	161

Microsoft	Microsoft Multiple E-Mail Client Address Spoofing	CVE-0000-0000	X	21/01/05	08/04/05	77
Microsoft	Microsoft Windows Message Queuing Service Stack Overflow Vulnerability	CVE-2007-3039	9	02/04/07	11/12/07	253
Microsoft	Microsoft Internet Explorer Element Tags Vulnerability	CVE-2007-5344	6,8	20/07/07	11/12/07	144
Microsoft	Microsoft Internet Explorer Node Manipulation Memory Corruption Vulnerability	CVE-2007-3903	6,8	22/05/07	11/12/07	203
Microsoft	Microsoft Internet Explorer setExpression Code Execution Vulnerability	CVE-2007-3902	9,3	20/07/07	11/12/07	144
Microsoft	Microsoft Windows DCERPC Authentication Denial of Service Vulnerability	CVE-2007-2228	7,8	05/02/07	10/10/07	247
Microsoft	Microsoft ISA Server SOCKS4 Proxy Connection Leakage Vulnerability	CVE-2007-4991	5	30/01/06	20/09/07	598
Microsoft	Microsoft Internet Explorer substringData Heap Overflow Vulnerability	CVE-2007-2223	9,3	03/10/06	14/08/07	315
Microsoft	Microsoft Windows Media Player Malformed Skin Header Code Execution Vulnerability	CVE-2007-3035	7,6	22/05/07	14/08/07	84
Microsoft	Microsoft Windows Media Player Skin Parsing Size Mismatch Heap Overflow Vulnerability	CVE-2007-3037	4	19/03/07	14/08/07	148
Microsoft	Microsoft Internet Explorer Prototype Dereference Code Execution Vulnerabilit	CVE-2007-1751	9,3	15/02/07	12/06/07	117
Microsoft	Microsoft Internet Explorer Language Pack Installation Remote Code Execution Vulnerability	CVE-2007-3027	9,3	08/11/06	12/06/07	216
Microsoft	Microsoft Internet Explorer Table Column Deletion Memory Corruption Vulnerability	CVE-2007-0944	9,3	03/10/06	08/05/07	217
Microsoft	Multiple Vendor Microsoft ATL/MFC ActiveX Type Confusion Vulnerability	CVE-2009-2494	10	05/12/08	11/08/09	249
Microsoft	Microsoft Office Web Components 2000 Buffer Overflow Vulnerability	CVE-2009-1534	9,3	17/03/08	11/08/09	512
Microsoft	Microsoft Internet Explorer HTML TIME 'ondatasetcomplete' Use After Free Vulnerability	CVE-2009-1917	9,3	06/05/09	28/07/09	83
Microsoft	Multiple Vendor Microsoft ATL/MFC ActiveX Security Bypass Vulnerability	CVE-2009-2493	9,3	05/12/08	11/08/09	249
Microsoft	Multiple Vendor Microsoft ATL/MFC ActiveX Information Disclosure Vulnerability	CVE-2009-2495	7,8	05/12/08	28/07/09	235
Microsoft	Microsoft Internet Explorer getElementsByTagName Memory Corruption Vulnerability	CVE-2009-1918	10	28/04/09	05/08/09	99
Microsoft	Microsoft Internet Explorer CSS Behavior Memory Corruption Vulnerability	CVE-2009-1919	9,3	28/04/09	05/08/09	99
Microsoft	Microsoft Windows WINS Service Heap Overflow Vulnerability	CVE-2009-1923	9,3	24/02/09	11/08/09	168
Microsoft	Microsoft Office OWC10.Spreadsheet ActiveX msDataSourceObject() Heap Corruption Vulnerability	CVE-2009-1136	9,3	19/03/07	11/08/09	876
Microsoft	Microsoft Office OWC10 ActiveX Control Loading and Unloading Heap Corruption Vulnerability	CVE-2009-0562	9,3	29/03/07	11/08/09	866
Microsoft	Microsoft Office OWC10.Spreadsheet ActiveX BorderAround() Heap Corruption Vulnerability	CVE-2009-2496	9,3	11/12/07	11/08/09	609

Microsoft	Microsoft Remote Desktop Client Arbitrary Code Execution Vulnerability	**CVE-2009-1133**	9,3	07/04/08	11/08/09	491
Microsoft	Microsoft Word 2000 WordPerfect 6.x Converter Stack Corruption Vulnerability	**CVE-2009-0088**	9,3	28/06/06	14/04/09	1021
Apple	Apple Mac OS X xnu Kernel workqueue_additem/workqueue_removeitem Index Validation Vulnerability	**CVE-2008-1517**	7,2	19/03/08	12/05/09	419
Apple	Apple QuickTime PICT Integer Overflow Vulnerability	**CVE-2008-3614**	6,8	13/05/08	09/09/08	119
Apple	Apple Mac OS X CoreGraphics PDF Type1 Font Integer Overflow Vulnerability	**CVE-2008-2322**	9,3	09/07/08	31/07/08	22
Apple	Apple Mac OS X mount_smbfs Stack Based Buffer Overflow Vulnerability	**CVE-2007-3876**	6,6	16/07/07	17/12/07	154
Apple	Apple Safari SVG Set.targetElement() Memory Corruption Vulnerability	**CVE-2009-1709**	9,3	10/11/08	08/06/09	210
Apple	Apple WebKit dir Attribute Freeing Dangling Object Pointer Vulnerability	**CVE-2009-1701**	9,3	09/02/09	08/06/09	119
Apple	Apple QuickTime Jpeg2000 Marker Size Heap Overflow Vulnerability	**CVE-2009-0957**	9,3	28/04/09	02/06/09	35
Apple	Apple QuickTime Packed-bit Decoding Heap Overflow Vulnerability	**CVE-2009-0952**	9,3	15/04/09	02/06/09	48
Apple	Apple OS X ATSServer Compact Font Format Parsing Memory Corruption Vulnerability	**CVE-2009-0154**	6,8	19/03/09	13/05/09	55
Apple	Apple QuickTime Macintosh Resource Processing Heap	**CVE-2008-0032**	5,8	13/09/07	15/01/08	124
Apple	Apple Mac OS X AppleTalk Socket IOCTL Kernel Stack Buffer Overflow	**CVE-2007-4267**	7,2	08/08/07	14/11/07	98
Apple	Apple Mac OS X AppleTalk mbuf Kernel Heap Overflow	**CVE-2007-4268**	7,2	08/08/07	14/11/07	98
Apple	Apple Mac OS X AppleTalk ASP Message Kernel Heap Overflow	**CVE-2007-4269**	7,2	08/08/07	14/11/07	98
Apple	Apple Mac OS X Mach Port Inheritance Privilege Escalation	**CVE-2007-3749**	7,2	07/09/07	14/11/07	68
Apple	Apple QuickTime Panorama Sample Atom Heap Buffer Overflow	**CVE-2007-4675**	9,3	13/09/07	05/11/07	53
Apple	Apple Mac OS X mDNSResponder HTTP Request Heap Overflow	**CVE-2007-3744**	5,8	26/07/07	07/08/07	12
Apple	Apple QuickTime SMIL File Processing Integer Overflow	**CVE-2007-2394**	9,3	02/04/07	11/07/07	100
Apple	Apple Computer Mac OS X pppd Plugin Loading Privilege Escalation	**CVE-2007-0752**	7,2	08/01/07	24/05/07	136
Apple	Apple Darwin Streaming Proxy Multiple Vulnerabilities	**CVE-2007-0748**	10	09/04/07	10/05/07	31
Apple	Apple QuickTime Color Table ID Heap Corruption	**CVE-2007-0718**	5,8	06/12/06	05/03/07	89
Apple	Apple QuickTime FLIC File Heap Overflow	**CAN-2006-4384**	5,1	16/08/06	12/09/06	27
Apple	Apple Mac OS X passwd Arbitrary Binary File Creation/Modification	**CVE-2005-2713**	6,8	23/08/05	03/02/06	164
Apple	Apple Mac OS X vpnd Server_id Buffer Overflow	**CAN-2005-1343**	7,2	25/04/05	04/05/05	9

Apple	Apple Mac OS X Server NeST -target Buffer Overflow	CAN-2005-0594	7,2	28/02/05	03/05/05	64
Apple	Apple iTunes Playlist Parsing Buffer Overflow	CAN-2005-0043	7,5	17/12/04	13/01/05	27
Apple	Apple Java CColourUIResource Pointer Dereference Code Execution Vulnerability	CVE-2009-1719	7,5	26/01/09	16/06/09	141
Apple	Apple WebKit attr() Invalid Attribute Memory Corruption Vulnerability	CVE-2009-1698	9,3	26/03/09	08/06/09	74
Apple	Apple Quicktime PICT Opcode 0x71 Heap Overflow Vulnerability	CVE-2009-0010	9,3	17/12/08	02/06/09	167
Apple	Apple Quicktime PICT Opcode 0x8201 Heap Overflow Vulnerability	CVE-2009-0953	9,3	17/12/08	02/06/09	167
Apple	Apple QuickTime CRGN Atom Parsing Heap Buffer Overflow Vulnerability	CVE-2009-0954	9,3	17/12/08	02/06/09	167
Apple	Apple Quicktime Picture Viewer FLC Delta-Encoded Frame Decompression Vulnerability	CVE-2009-0951	9,3	28/10/08	02/06/09	217
Apple	Apple OS X ATSServer Compact Font Format Parsing Memory Corruption Vulnerability	CVE-2009-0154	6,8	19/03/09	13/05/09	55
Apple	Apple Safari Malformed SVGList Parsing Code Execution Vulnerability	CVE-2009-0945	9,3	19/03/09	13/05/09	55
Apple	Apple QuickTime PICT Unspecified Tag Heap Overflow Vulnerability	CVE-2009-0010	9,3	15/04/09	13/05/09	28
Apple	Apple QuickTime STSD JPEG Atom Heap Corruption Vulnerability	CVE-2009-0007	9,3	25/06/08	21/01/09	210
Apple	Apple QuickTime Cinepak Codec MDAT Heap Corruption Vulnerability	CVE-2009-0006	9,3	23/06/08	21/01/09	212
Apple	Apple QuickTime AVI Header nBlockAlign Heap Corruption Vulnerability	CVE-2009-0003	9,3	15/10/08	21/01/09	98
Apple	Apple QuickTime VR Track Header Atom Heap Corruption Vulnerability	CVE-2009-0002	9,3	16/09/08	21/01/09	127
Apple	Apple CUPS HP-GL/2 Filter Remote Code Execution Vulnerability	CVE-2008-3641	10	19/08/08	09/10/08	51
Apple	Apple QuickTime MDAT Frame Parsing Memory Corruption Vulnerability	CVE-2008-3627	9,3	19/05/08	09/09/08	113
Apple	Apple QuickTime Player H.264 Parsing Heap Corruption Vulnerability	CVE-2008-3627	9,3	13/05/08	09/09/08	119
Apple	Apple QuickTime AVC1 Atom Parsing Heap Overflow Vulnerability	CVE-2008-3627	9,3	15/05/08	09/09/08	117
Apple	Apple QuickTime STSZ Atom Parsing Heap Corruption Vulnerability	CVE-2008-3626	6,8	15/05/08	09/09/08	117
Apple	Apple QuickTime Panorama PDAT Atom Parsing Buffer Overflow Vulnerability	CVE-2008-3625	9,3	25/06/08	09/09/08	76
Apple	Apple QuickTime IV32 Codec Parsing Stack Overflow Vulnerability	CVE-2008-3635	9,3	19/08/08	09/09/08	21
Apple	Apple Safari StyleSheet ownerNode Heap Corruption Vulnerability	CVE-2008-2317	9,3	13/05/08	25/07/08	73
Apple	Apple QuickTime SMIL qtnext Redirect File Execution Vulnerability	CVE-2008-1585	6,8	08/05/08	10/06/08	33
Apple	Apple QuickTime Indeo Video Buffer Overflow Vulnerability	CVE-2008-1584	6,8	07/02/08	10/06/08	124

Apple	Apple Safari WebKit PCRE Handling Integer Overflow Vulnerability	**CVE-2008-1026**	6,8	27/03/08	16/04/08	20
Apple	Apple QuickTime Malformed VR obji Atom Parsing Memory Corruption Vulnerability	**CVE-2008-1022**	6,8	07/02/08	03/04/08	56
Apple	Apple QuickTime Run Length Encoding Heap Overflow Vulnerability	**CVE-2008-1021**	6,8	07/02/08	03/04/08	56
Apple	Apple QuickTime Kodak Encoding Heap Overflow Vulnerability	**CVE-2008-1020**	6,8	07/02/08	03/04/08	56
Apple	Apple QuickTime MP4A Atom Parsing Heap Corruption Vulnerability	**CVE-2008-1018**	6,8	07/02/08	03/04/08	56
Apple	Apple QuickTime Clipping Region Heap Overflow Vulnerability	**CVE-2008-1017**	6,8	07/02/08	03/04/08	56
Apple	Apple Quicktime Multiple Opcode Memory Corruption Vulnerabilities	**CVE-2008-1019**	6,8	07/02/08	03/04/08	56
Apple	Apple QuickTime Uncompressedfile Opcode Stack Overflow Vulnerability	**CVE-2007-4672**	7,6	14/09/07	05/11/07	52
Apple	Apple QuickTime PICT File Poly Opcodes Heap Corruption Vulnerability	**CVE-2007-4676**	9,3	14/09/07	05/11/07	52
Apple	Apple Quicktime PICT File PackBitsRgn Parsing Heap Corruption Vulnerability	**CVE-2007-4676**	9,3	14/09/07	05/11/07	52
Apple	Apple QuickTime Color Table RGB Parsing Heap Corruption Vulnerability	**CVE-2007-4677**	9,3	14/09/07	05/11/07	52
Apple	Apple QTJava toQTPointer() Pointer Arithmetic Memory Overwrite Vulnerability	**CVE-2007-2175**	7,6	23/04/07	01/05/07	8
Apple	Apple Quicktime UDTA Parsing Heap Overflow Vulnerability	**CVE-2007-0714**	9,3	14/08/06	07/03/07	205
IBM	IBM AIX libc MALLOCDEBUG File Overwrite Vulnerability	**CVE-0000-0000**	X	05/01/08	19/05/09	500
IBM	IBM AIX muxatmd Buffer Overflow	**CVE-0000-0000**	X	16/12/08	15/04/09	120
IBM	IBM Tivoli Storage Manager Express Heap Buffer Overflow Vulnerability	**CVE-2008-4563**	10	22/07/08	03/10/09	438
IBM	IBM DB2 Universal Database Administration Server File Creation Vulnerability	**CVE-2007-5664**	6,9	03/10/07	09/04/08	189
IBM	IBM DB2 Universal Database db2dasStartStopFMDaemon Buffer Overflow Vulnerability	**CVE-2007-5758**	6,9	29/11/07	09/04/08	132
IBM	IBM Informix Dynamic Server SQLIDEBUG File Creation Vulnerability	**CVE-2008-0369**	6,9	01/09/07	31/01/08	152
IBM	IBM AIX pioout BSS Buffer Overflow Vulnerability	**CVE-2007-5764**	7,2	29/11/07	23/01/08	55
IBM	IBM Tivoli PMfOSD HTTP Request Method Buffer Overflow Vulnerability	**CVE-2008-0401**	10	24/10/07	22/01/08	90
IBM	IBM DB2 Universal Database db2pd Arbitrary Library Loading Vulnerability	**CVE-2007-5757**	6,9	22/03/07	07/02/08	322
IBM	IBM Tivoli Storage Manager Express for Microsoft SQL Heap Overflow Vulnerability	**CVE-2008-4801**	10	12/05/08	30/10/08	171
IBM	IBM Lotus Sametime Community Services	**CVE-2008-2499**	7,5	11/12/07	21/05/08	162
IBM	IBM Informix Dynamic Server Authentication Password Stack Overflow	**CVE-2008-0727**	8,5	07/11/07	13/03/08	127

IBM	IBM Informix Dynamic Server DBPATH Buffer Overflow	CVE-2008-0727	8,5	07/11/07	13/03/08	127
IBM	IBM Tivoli Storage Manager Express Backup Server Heap Overflow	CVE-2008-0247	10	05/12/07	14/01/08	40
IBM	IBM DB2 DB2JDS Multiple Vulnerabilities	CVE-2007-2582	10	09/11/06	10/10/07	335
IBM	IBM Tivoli Storage Manager Express CAD Service Buffer Overflow	CVE-2007-4880	10	22/05/07	24/09/07	125
IBM	IBM Tivoli Monitoring Express Universal Agent Heap Overflow	CVE-2007-2137	10	14/09/06	17/04/07	215
IBM	IBM Lotus Domino IMAP Server CRAM-MD5 Authentication Buffer Overflow	CVE-2007-1675	10	31/08/06	28/03/07	209
IBM	IBM Lotus Domino Server Web Service DoS Vulnerability	CVE-0000-0000	X	07/02/05	06/04/05	58
IBM	IBM AIX lspath Local File Access	CAN-2005-0262	7,2	21/12/04	10/02/05	51
IBM	IBM AIX ipl_varyon Local Buffer Overflow	CAN-2005-0262	7,2	21/12/04	10/02/05	51
IBM	IBM AIX netpmon Local Buffer Overflow Vulnerability	CAN-2005-0263	7,2	21/12/04	10/02/05	51
IBM	IBM AIX auditselect Local Format String	CAN-2005-0250	7,2	21/12/04	08/02/05	49
IBM	IBM AIX chdev Local Format String	CAN-2005-0240	7,2	21/12/04	07/02/05	48
IBM	IBM Lotus Domino 7 tunekrnl Multiple Vulnerabilities	CVE-0000-0000	X	15/08/06	08/11/06	85
IBM	IBM Lotus Domino Server LDAP DoS	CAN-2005-2712	7,8	23/08/05	10/02/06	171
IBM	IBM Informix Dynamic Server DBLANG Directory Traversal	CVE-2007-5670	X	01/09/07	09/11/07	69
IBM	IBM AIX swcons Local Arbitrary File Acces	CVE-0000-0000	X	21/12/04	30/10/07	1043
IBM	IBM AIX 5.2 crontab BSS Buffer Overflow	CVE-2007-4621	7,2	29/08/07	30/10/07	62
IBM	IBM AIX dig dns_name_fromtext Integer Underflow	CVE-2007-4622	7,2	30/08/07	30/10/07	62
IBM	IBM AIX lqueryvg Stack Buffer Overflow	CVE-2007-4513	7,2	21/08/07	30/10/07	70
IBM	IBM AIX ftp domacro Parameter Buffer Overflow	CVE-2007-4217	7,2	15/08/07	30/10/07	76
IBM	IBM AIX bellmail Stack Buffer Overflow Vulnerability	CVE-2007-4623	7,2	28/08/07	30/10/07	63
IBM	IBM Lotus Notes Client TagAttributeListCopy Buffer Overflow	CVE-2007-4222	9,3	07/02/07	23/10/07	258
IBM	IBM Lotus Domino IMAP Buffer Overflow	CVE-2007-3510	9	27/06/07	23/10/07	118
IBM	IBM DB2 Universal Database Multiple Race Condition	CVE-2007-4270	6,9	22/03/07	16/08/07	147
IBM	IBM DB2 Universal Database Directory Traversal	CVE-2007-4271	2,1	22/03/07	16/08/07	147

IBM	IBM DB2 Universal Database Multiple File Creation	CVE-2007-4272	1,9	22/03/07	16/08/07	147
IBM	IBM DB2 Universal Database Directory Creation	CVE-2007-4273	4,6	22/03/07	16/08/07	147
IBM	IBM DB2 Universal Database Multiple Untrusted Search Path	CVE-2007-4275	6,9	23/03/07	16/08/07	146
IBM	IBM DB2 Universal Database buildDasPaths Buffer Overflow	CVE-2007-4276	1,9	22/03/07	16/08/07	147
IBM	IBM AIX pioout Arbitrary Library Loading	CVE-2007-4003	6,9	05/06/07	26/07/07	51
IBM	IBM AIX capture Terminal Control Sequence Buffer Overflow	CVE-2007-3333	6,9	05/06/07	26/07/07	51
IBM	IBM AIX ftp gets() Multiple Buffer Overflow	CVE-0000-0000	X	05/06/07	26/07/07	51
IBM	IBM Tivoli Provisioning Manager for OS Deployment TFTP Blocksize DoS	CVE-2007-3268	5	19/06/07	17/07/07	28
IBM	IBM AIX libodm ODMPATH Stack Overflow	CVE-0000-0000	X	02/04/07	09/07/07	98
IBM	IBM Tivoli Provisioning Manager for OS Deployment Multiple	CVE-0000-0000	X	30/01/07	31/03/07	60
IBM	IBM Lotus Sametime JNILoader Arbitrary DLL Load	CVE-0000-0000	X	01/08/06	29/03/07	240
IBM	IBM Lotus Domino Web Access Cross Site Scripting	CVE-2006-4843	4,3	17/08/06	28/03/07	223
IBM	IBM Lotus Domino Server LDAP Request Invalid DN Message Heap Overflow	CVE-0000-0000	X	09/10/06	28/03/07	170
IBM	IBM DB2 Universal Database DB2INSTANCE File Creation	CVE-0000-0000	X	15/11/06	22/02/07	99
IBM	IBM DB2 Universal Database Multiple Privilege Escalation	CVE-0000-0000	X	15/11/06	22/02/07	99
IBM	IBM DB2 Universal Database Administration Server Memory Corruption	CVE-2007-5664	6,9	18/06/07	07/02/08	234
IBM	IBM Informix Dynamic Server onedcu File Creation	CVE-2008-0368	7,2	01/09/07	31/01/08	152
IBM	IBM AIX libC _LIB_INIT_DBG Arbitrary File Creation Vulnerability	CVE-0000-0000	X	25/02/09	04/08/09	160
IBM	IBM Lotus Sametime Community Services Multiplexer Stack Overflow	CVE-2008-2499	7,5	11/12/07	21/05/08	162
CA	Computer Associates Alert Notification Service Multiple RPC Buffer Overflow Vulnerabilities	CVE-2007-4620	9	24/08/07	03/04/08	223
CA	CA ARCserve Backup for Laptops and Desktops Authentication Bypass Vulnerability	CVE-2007-5002	X	06/03/07	20/09/07	198
CA	CA ARCServe Backup for Laptops and Desktops Multiple Buffer Overflow	CVE-2007-5003	10	21/03/07	20/09/07	183
CA	Computer Associates BrightStor HSM r11.5 Multiple Vulnerabilities	CVE-2007-5082	10	13/04/07	27/09/07	167
CA	Computer Associates AntiVirus CHM File Handling DoS Vulnerability	CVE-2007-3875	4,3	16/01/07	24/07/07	189
CA	Computer Associates eTrust Intrusion Detection CallCode ActiveX Control Code Execution Vulnerability	CVE-2007-3302	9,3	20/06/07	24/07/07	34

CA	Computer Associates Alert Notification Server Multiple Buffer Overflow	CVE-2007-3825	9,3	27/02/07	17/07/07	140
CA	Computer Associates eTrust InoTask.exe Antivirus Buffer Overflow	CVE-2007-2523	7,2	07/02/07	09/05/07	91
CA	Computer Associates eTrust Intrusion Detection Denial of Service	CVE-0000-0000	X	16/01/07	27/02/07	42
CA	Computer Associates BrightStor ARCserve Backup RPC Engine PFC Request Buffer Overflow	CVE-2007-0169	7,5	03/01/07	11/01/07	8
CA	Computer Associates iTechnology iGateway Service Content-Length Buffer Overflow	CVE-2005-3653	10	15/11/05	23/01/06	69
CA	CA BrightStor ARCserve Backup Agent for MS SQL Server Buffer Overflow	CAN-2005-1272	7,5	25/04/05	02/08/05	99
CA	CA BrightStor ARCserve Backup v11 Discovery Service Remote Buffer Overflow	CAN-2005-0260	10	12/11/04	09/02/05	89
CA	Computer Associates BrightStor ARCserve Backup UniversalAgent Buffer Overflow	CAN-2005-1018	7,5	02/12/04	11/04/05	130
CA	Computer Associates eTrust Intrusion Detection System CPImportKey DoS Vulnerability	CAN-2005-0968	5	02/12/04	05/04/05	124
CA	Computer Associates License Client and Server Invalid Command Buffer Overflow	CAN-2005-0581	4,6	08/02/05	02/03/05	22
CA	Computer Associates License Client PUTOLF Buffer Overflow	CAN-2005-0582	10	08/02/05	02/03/05	22
CA	Computer Associates License Client PUTOLF Directory Traversal	CAN-2005-0583	5	08/02/05	02/03/05	22
CA	Computer Associates License Client/Server GETCONFIG Buffer Overflow	CAN-2005-0581	4,6	01/12/04	02/03/05	91
CA	Computer Associates License Client/Server GCR Network Buffer Overflow	CAN-2005-0581	4,6	01/12/04	02/03/05	91
CA	Computer Associates License Client/Server GCR Checksum Buffer Overflow	CAN-2005-0581	4,6	01/12/04	02/03/05	91
CA	Computer Associates BrightStor ARCserve Backup UniversalAgent Backdoor	CAN-2005-0349	7,5	02/12/04	10/02/05	70
CA	CA Multiple Product Message Engine RPC Server Code Execution Vulnerability	CVE-2006-5143	7,5	07/04/06	05/10/06	181
CA	CA BrightStor ARCserve Discovery Service Remote Buffer Overflow Vulnerability	CVE-2006-5143	7,5	07/04/06	05/10/06	181
CA	CA BrightStor ARCserve Backup Message Engine Insecure Method Exposure Vulnerability	CVE-2007-5328	10	12/01/07	26/11/07	318
CA	CA Multiple Product AV Engine CAB Header Parsing Stack Overflow Vulnerability	CVE-2007-2864	9,3	16/02/07	05/06/07	109
CA	CA Multiple Product AV Engine CAB Filename Parsing Stack Overflow Vulnerability	CVE-2007-2863	10	08/11/06	05/06/07	209
CA	CA eTrust AntiVirus Server inoweb Buffer Overflow Vulnerability	CVE-2007-2522	10	06/11/06	10/05/07	185
CA	CA BrightStor ArcServe Media Server Multiple Buffer Overflow Vulnerabilities	CVE-2007-2139	10	08/03/07	24/04/07	47
CA	CA BrightStor ARCserve Backup Tape Engine Buffer Overflow Vulnerability	CVE-2007-0169	7,5	08/11/06	11/01/07	64
CA	CA BrightStor ARCserve Backup Message Engine Buffer Overflow Vulnerability	CVE-2007-0169	7,5	08/11/06	11/01/07	64

CA	CA BrightStor ARCserve Backup Tape Engine Code Execution Vulnerability	CVE-2007-0168	7,5	01/11/06	11/01/07	71
CA	CA ETrust Secure Content Manager Gateway FTP LIST Stack Overflow Vulnerability	CVE-2008-2541	10	23/05/08	04/06/08	12
CA	CA ETrust Secure Content Manager Gateway FTP PASV Stack Overflow Vulnerability	CVE-2008-2541	10	23/05/08	04/06/08	12
CA	CA BrightStor ARCserve Backup caloggerd Arbitrary File Writing Vulnerability	CVE-2008-2241	10	12/09/06	19/05/08	615
CA	CA Unicenter Software Delivery dtscore.dll Stack Overflow Vulnerability	CVE-0000-0000	X	14/09/07	07/08/09	695
Symantec	Symantec System Center Alert Management System Console Arbitrary Program Execution Design Error Vulnerability	CVE-2009-1431	9,3	09/10/07	28/04/09	567
Symantec	Symantec Norton Internet Security 2008 ActiveX Control Buffer Overflow Vulnerability	CVE-2008-0312	9,3	05/12/07	02/04/08	119
Symantec	Symantec Internet Security 2008 ActiveDataInfo.LaunchProcess Design Error Vulnerability	CVE-2008-0313	6,8	14/12/07	02/04/08	110
Symantec	Symantec Scan Engine 5.1.2 RAR File Buffer Overflow Vulnerability	CVE-2008-0309	6,8	14/06/07	26/02/08	257
Symantec	Symantec Veritas Storage Foundation Scheduler Service DoS Vulnerability	CVE-2007-4516	4,3	15/08/07	20/02/08	189
Symantec	Symantec Altiris Deployment Solution TFTP/MTFTP Service Directory Traversal Vulnerability	CVE-2007-3874	7,8	13/07/07	31/10/07	110
Symantec	Symantec Backup Exec RPC Remote Heap Overflow Vulnerability	CVE-2007-3509	7,5	01/05/07	11/07/07	71
Symantec	Symantec AntiVirus symtdi.sys Local Privilege Escalation Vulnerability	CVE-0000-0000	X	10/01/07	11/07/07	182
Symantec	Symantec Norton Internet Security 2006 COM Object Security ByPass Vulnerability	CVE-2006-3456	8,5	13/12/06	09/05/07	147
Symantec	Symantec Norton Ghost 10 Service Manager Buffer Overflow Vulnerability	CVE-0000-0000	X	02/01/07	26/04/07	114
Symantec	Symantec Scan Engine 5.1.2 RAR File Denial of Service	CVE-2008-0308	7,1	14/06/07	26/02/08	257
Symantec	Symantec Ghost Multiple Denial of Service	CVE-0000-0000	X	13/12/06	05/06/07	174
Symantec	Symantec VERITAS Storage Foundation Administration Service DoS	CVE-2007-1593	5	11/10/06	01/06/07	233
Symantec	Symantec Norton Ghost 10 Recovery Points Insecure Password Storage Vulnerability	CVE-0000-0000	X	02/01/07	26/04/07	114
Symantec	Symantec AntiVirus IOCTL Kernel Privilege Escalation	CVE-2006-4927	4,6	19/09/06	05/10/06	16
Symantec	Symantec Norton AntiVirus LiveUpdate Local Privilege Escalation	CVE-2005-2759	7,2	31/08/05	20/10/05	50
Symantec	Symantec Norton AntiVirus DiskMountNotify Local Privilege Escalation	CVE-2005-3270	7,2	31/08/05	20/10/05	50
Symantec	Symantec AntiVirus Scan Engine Web Service Buffer Overflow	CAN-2005-2758	10	31/08/05	04/10/05	34
Symantec	Symantec AntiVirus 9 Corporate Edition Local Privilege Escalation	CAN-2005-2017	10	15/06/05	29/08/05	75

Symantec	Symantec Veritas NetBackup CONNECT_OPTIONS Buffer Overflow Vulnerability	**CVE-2006-5822**	10	14/08/06	13/12/06	121
Symantec	Symantec Veritas NetBackup Long Request Buffer Overflow Vulnerability	**CVE-2006-6222**	10	14/08/06	13/12/06	121
Symantec	Symantec VERITAS NetBackup Database Manager Buffer Overflow Vulnerability	**CVE-2006-0990**	9	24/01/06	27/03/06	62
Symantec	Symantec VERITAS NetBackup Volume Manager Buffer Overflow Vulnerability	**CVE-2006-0989**	9	20/12/05	27/03/06	97
Symantec	Symantec AntiVirus Engine CAB Parsing Heap Overflow Vulnerability	**CVE-2007-0447**	9,3	09/11/06	12/07/07	245
Symantec	Symantec AntiVirus Engine RAR File Parsing DoS Vulnerability	**CVE-2007-3699**	9,3	01/11/06	12/07/07	253
Symantec	Symantec Veritas Storage Foundation Scheduler Service NULL Session Authentication Bypass Vulnerability	**CVE-2008-3703**	10	26/06/08	14/08/08	49
Symantec	Symantec Altiris Deployment Solution Domain Credential Disclosure Vulnerability	**CVE-2008-2291**	7,5	07/02/08	15/05/08	98
Symantec	Symantec Altiris Deployment Solution SQL Injection Vulnerability	**CVE-2008-2286**	7,5	07/02/08	15/05/08	98
Symantec	Symantec VERITAS Storage Foundation Administrator Service Heap Overflow Vulnerability	**CVE-2008-0638**	9,3	14/09/07	20/02/08	159
Symantec	Symantec Backup Exec Remote File Upload Vulnerability	**CVE-2008-0457**	10	11/12/07	06/02/08	57
Oracle	Oracle Database 10g R2 Summary Advisor Arbitrary File Rewrite Vulnerability	**CVE-2008-3997**	4	24/03/08	12/01/09	294
Oracle	Oracle Secure Backup Administration Server login.php Command Injection Vulnerability	**CVE-2008-4006**	10	18/07/08	13/01/09	179
Oracle	Oracle Secure Backup Administration Server login.php Command Injection Vulnerability	**CVE-2008-5449**	10	08/03/07	13/01/09	677
Oracle	Oracle WebLogic Apache Connector	**CVE-2008-4008**	10	31/07/08	29/10/08	90
Oracle	Oracle Internet Directory Pre-Authentication LDAP DoS Vulnerability	**CVE-2008-2595**	5	11/05/07	15/07/08	431
Oracle	Oracle Database DBMS_AQELM Package Buffer Overflow Vulnerability	**CVE-2008-2607**	6,5	18/12/07	15/07/08	210
Oracle	Oracle Database Local Untrusted Library Path Vulnerability	**CVE-2008-2613**	6,5	25/01/08	15/07/08	172
Oracle	Oracle Application Express Privilege Escalation Vulnerability	**CVE-2008-1811**	10	18/01/08	15/04/08	88
Oracle	Oracle E-Business Suite Business Intelligence SQL Injection Vulnerability	**CVE-0000-0000**	X	29/01/07	16/12/08	687
Oracle	Oracle Applications Server 10g Format String Vulnerability	**CVE-0000-0000**	X	07/11/07	14/04/09	524
Oracle	Oracle TimesTen evtdump Remote Format String Vulnerability	**CVE-2008-5440**	7,5	07/04/08	14/01/09	282
Oracle	Oracle Secure Backup exec_qr() Command Injection Vulnerability	**CVE-2008-5448**	10	13/07/07	14/01/09	551
Oracle	Oracle E-Business Suite SQL Injection Vulnerability	**CVE-2007-5766**	7,5	29/01/07	31/10/07	275

Oracle	Oracle E-Business Suite Arbitrary Document Download Vulnerability	**CVE-2007-2135**	7,8	29/01/07	18/04/07	79
Oracle	Oracle Secure Backup Administration Server Authentication Bypass Vulnerability	**CVE-2009-1977**	10	26/03/09	18/08/09	145
Oracle	Oracle Secure Backup Administration Server Multiple Command Injection Vulnerabilities	**CVE-2009-1978**	9	26/03/09	18/08/09	145
Adobe	Adobe Reader and Acrobat FlateDecode Integer Overflow Vulnerability	**CVE-2009-1856**	9,3	25/02/09	06/09/09	193
Adobe	Adobe Reader and Acrobat JBIG2 Encoded Stream Heap Overflow Vulnerability	**CVE-2009-0928**	7,5	24/02/09	24/03/09	28
Adobe	Adobe Flash Player Invalid Object Reference Vulnerability	**CVE-2009-0520**	9,3	25/08/08	24/02/09	183
Adobe	Adobe Reader Embedded Font Handling Out of Bounds Array Indexing Vulnerability	**CVE-2008-4812**	9,3	27/12/07	04/11/08	313
Adobe	Adobe Acrobat Professional And Reader AcroJS Heap Corruption Vulnerability	**CVE-2008-4817**	9,3	21/03/08	04/11/08	228
Adobe	Adobe Flash Media Server 2 Multiple Integer Overflow Vulnerabilities	**CVE-2007-6149**	10	27/11/07	02/12/08	381
Adobe	Adobe Reader and Acrobat Multiple Stack-based Buffer Overflow Vulnerabilities	**CVE-2007-5659**	9,3	10/10/07	08/02/08	121
Adobe	Adobe Reader and Acrobat JavaScript Insecure Method Exposure Vulnerability	**CVE-2007-5663**	9,3	03/10/07	08/02/08	128
Adobe	Adobe Shockwave Player Director File Parsing Pointer Overwrite Vulnerability	**CVE-2009-1860**	9,3	12/05/08	24/06/09	408
Adobe	Adobe Reader U3D RHAdobeMeta Stack Overflow Vulnerability	**CVE-2009-1855**	9,3	24/02/09	10/06/09	106
Adobe	Adobe PageMaker Key Strings Stack Buffer Overflow Vulnerability	**CVE-2008-6432**	9,3	18/12/07	29/10/08	316
Adobe	Adobe Flash Media Server 2 Memory Corruption	**CVE-2007-6148**	10	27/11/07	12/02/08	77
Adobe	Adobe Reader Security Provider Unsafe Libary Path	**CVE-2007-5666**	6,2	25/09/07	08/02/08	136
Adobe	Adobe Reader and Acrobat JavaScript Insecure Method Exposure	**CVE-2007-5663**	9,3	03/10/07	08/02/08	128
Adobe	Adobe Macromedia ColdFusion MX7 Insecure File Permissions	**CVE-2007-1874**	7,2	21/03/07	10/04/07	20
Adobe	Adobe Macromedia ColdFusion Source Code Disclosure	**CVE-2006-5858**	5	08/11/06	09/01/07	62
Adobe	Adobe Version Cue VCNative Arbitrary File Overwrite	**CAN-2005-1842**	2,1	27/06/05	29/08/05	63
Adobe	Adobe Version Cue VCNative Arbitrary Library Loading	**CAN-2005-1843**	4,6	27/06/05	29/08/05	63
Adobe	Adobe Acrobat Reader UnixAppOpenFilePerform() Buffer Overflow	**CAN-2005-1625**	5	12/05/05	05/07/05	54
Adobe	Adobe Acrobat getIcon() Stack Overflow	**CVE-2009-0927**	10	03/07/08	24/03/09	264
Adobe	Adobe Acrobat PDF Javascript getCosObj Memory Corruption	**CVE-2008-4813**	9,3	12/05/08	04/11/08	176
Adobe	Adobe Acrobat Reader Malformed PDF Code Execution	**CVE-2008-4813**	9,3	08/04/08	04/11/08	210

Adobe	Adobe Acrobat PDF Javascript printf Stack Overflow	**CVE-2008-2992**	9,3	21/01/08	04/11/08	288
Adobe	Adobe Flash DefineSceneAndFrameLabelData Parsing Memory Corruption	**CVE-2007-0071**	9,3	07/02/08	22/05/08	105
Adobe	Adobe Flash Player DeclareFunction2 Invalid Object Use	**CVE-2007-6019**	9,3	07/02/08	08/04/08	61
Adobe	Adobe Acrobat Javascript for PDF Integer Overflow	**CVE-2008-0726**	9,3	14/11/07	11/02/08	89
Adobe	Adobe Download Manager AOM Parsing Buffer Overflow	**CVE-2006-5856**	6,8	07/04/06	06/12/06	243
Adobe	Adobe Macromedia ShockWave Code Execution	**CVE-2005-3525**	9,3	22/11/05	23/02/06	93
Adobe	Adobe Flash Player Invalid Loader Object Reference Vulnerability	**CVE-2009-1864**	9,3	25/08/08	30/07/09	339
Adobe	Adobe Flash Player URL Parsing Heap Overflow Vulnerability	**CVE-2009-1868**	9,3	09/04/09	06/08/09	119