

# SISTEMA DE ALERTAS

## MANUAL DE USUARIO

*Versión 0.9*

JULIO 2014

## Contenido

Índice de Figuras .....	2
Introducción .....	3
Acceso a la aplicación** .....	3
Módulo Administrativo .....	4
Actualizaciones.....	4
Vulnerabilidades.....	5
Vulnerabilidades más recientes .....	5
Archivo de Vulnerabilidades .....	7
Software Soportado .....	10
Escaneo .....	12

## Índice de Figuras

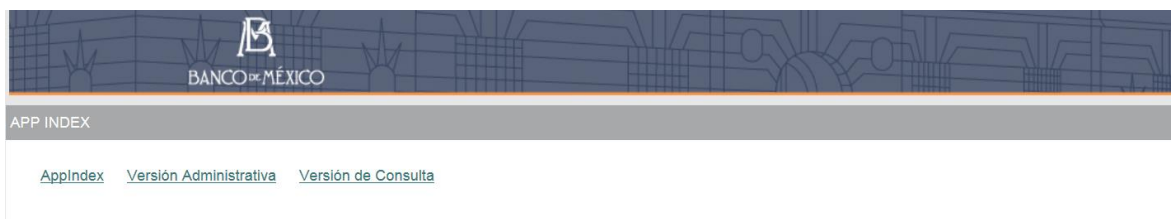
Figura 1 Pantalla de Inicio .....	3
Figura 2 Barra de Navegación Administrativa .....	3
Figura 3 Menú desplegable de configuración .....	4
Figura 4 Tabla de Fuentes de la Aplicación .....	4
Figura 5 Menú desplegable de vulnerabilidades .....	5
Figura 6 Tabla de Vulnerabilidades más recientes.....	6
Figura 7 Detalle de una vulnerabilidad .....	7
Figura 8 Menú desplegable de vulnerabilidades .....	7
Figura 9 Tabla de archivo de vulnerabilidades.....	8
Figura 10 Barra de búsqueda .....	9
Figura 11 Resultados de la búsqueda.....	9
Figura 12 Menú desplegable de vulnerabilidades .....	10
Figura 13 Tabla de software soportado .....	10
Figura 14 Barra de búsqueda de software .....	11
Figura 15 Resultados de búsqueda de software .....	11
Figura 16 Pantalla de Escaneo.....	12
Figura 17 Selección de fechas de escaneo .....	13
Figura 18 Botón de Escaneo .....	13
Figura 19 Resultados del escaneo .....	14
Figura 20 Botón de exportación.....	15
Figura 21 Resultados en formato de texto.....	15

## Introducción

Este manual tiene como objetivo demostrar la manera en que se utilizan las funcionalidades básicas de la aplicación de alertas.

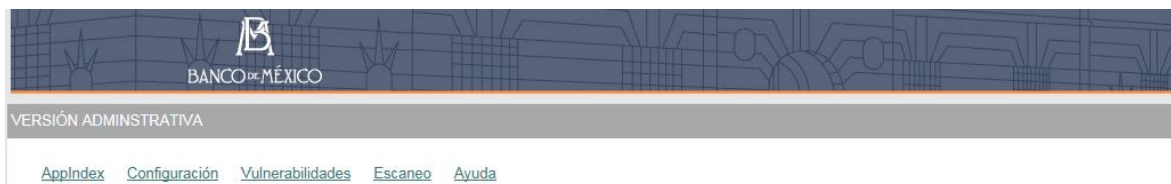
### Acceso a la aplicación\*\*

Para comenzar a utilizar la aplicación se debe acceder a través del navegador web de la ETB, preferiblemente Internet Explorer 10+, a la dirección del servidor de aplicaciones donde se encuentra contenida la misma: <https://localhost:8080/sisalbm/>.



*Figura 1 Pantalla de Inicio*

Dentro de la versión administrativa se encuentra la siguiente barra de navegación, la cual permite explorar las diferentes opciones de la aplicación:



*Figura 2 Barra de Navegación Administrativa*

## Módulo Administrativo

Dentro de este módulo se contemplan las siguientes tareas:

- Actualización de la aplicación
- Consulta de Vulnerabilidades
- Manejo de inventario de software
- Realización de escaneos

## Actualizaciones

La aplicación obtiene la información de vulnerabilidades del sitio: <http://nvd.nist.gov>, el cual ofrece documentos en formato XML, los cuales contienen información más reciente o histórica de las vulnerabilidades que surgen día a día.


La aplicación cuenta con un parser que se encarga de convertir toda esa información en forma de objetos, para su fácil manejo y presentación al usuario.

En esta primera versión de la aplicación, la actualización de esa información debe ser manual por parte del usuario, para poder realizar está actualización hay que ubicar en la barra de navegación, el menú configuración y posteriormente seleccionar la opción [Administrar Fuentes] del menú desplegable.



Figura 3 Menú desplegable de configuración







Una vez realizado esto, se mostrara la siguiente pantalla, la cual contiene la URL del archivo ya sea de vulnerabilidades recientes o históricas, además de la última fecha de actualización y los enlaces con las opciones correspondientes.


**BANCO de MÉXICO**


**VERSIÓN ADMINISTRATIVA**

[AppIndex](#)
[Configuración](#)
[Vulnerabilidades](#)
[Escaneo](#)
[Ayuda](#)

**FUENTES DE LA APLICACIÓN**

Nombre	URL	Ultima Actualización	Opciones
Vulnerabilidades Recientes	<a href="http://nvd.nist.gov/download/nvdcve-recent.xml">http://nvd.nist.gov/download/nvdcve-recent.xml</a>	22 de julio de 2014	 
Archivo de Vulnerabilidades	<a href="http://nvd.nist.gov/download/nvdcve-2014.xml">http://nvd.nist.gov/download/nvdcve-2014.xml</a>	22 de julio de 2014	 
Prueba de Enlace	<a href="http://nvd.nist.gov/download/nvdcve-modified.xml">http://nvd.nist.gov/download/nvdcve-modified.xml</a>	16 de julio de 2014	 

*Figura 4 Tabla de Fuentes de la Aplicación*

Para iniciar con la actualización se debe hacer clic en el icono  que se encuentra situado al final de la fila de la fuente que se desee actualizar.

La aplicación mostrara la siguiente notificación en la parte inferior derecha.

[IMG]

Una vez realizada la actualización, se desplegará el siguiente mensaje, indicando que la fuente fue actualizada.

## Vulnerabilidades

Dentro del apartado de vulnerabilidades se contemplan 2 tipos de vulnerabilidades:

- Vulnerabilidades recientes

Las cuales contemplan un periodo no mayor a 8 días, a partir del día actual, por ejemplo, si el día actual es 20 de Julio, las vulnerabilidades recientes pueden empezar del 12 de Julio en adelante.

- Archivo de Vulnerabilidades

Contiene vulnerabilidades desde el 1er día del año, hasta el día actual o en su defecto, algunos días anteriores a la fecha actual.

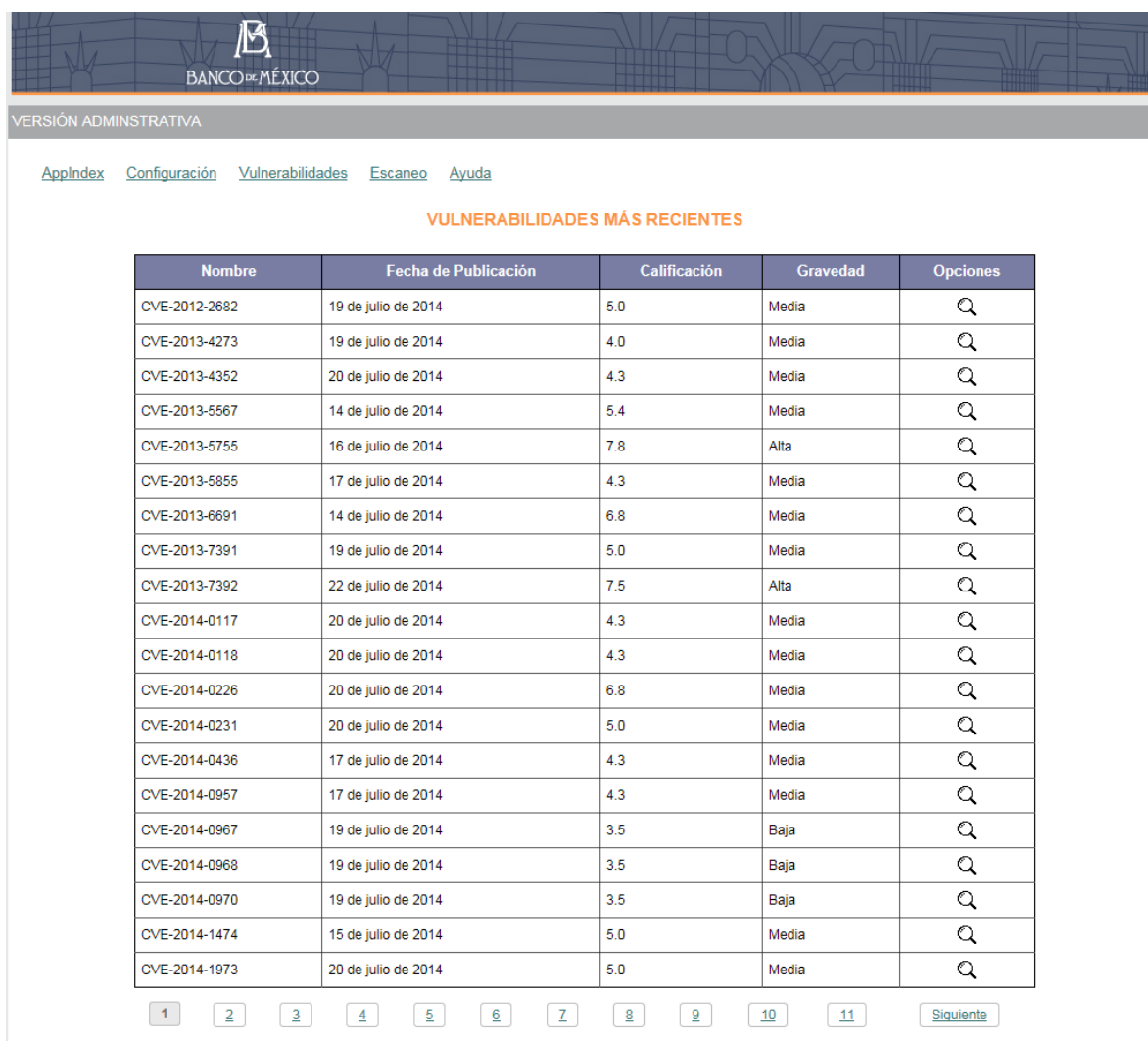
## Vulnerabilidades más recientes

Para poder consultar las vulnerabilidades recientes, hay que ubicar en la barra de navegación el apartado Vulnerabilidades y seleccionar a opción 'Más Recientes' dentro del menú desplegable.



Figura 5 Menú desplegable de vulnerabilidades

Al seleccionar está opción se mostrara la siguiente pantalla:



VERSIÓN ADMINISTRATIVA

[AppIndex](#) [Configuración](#) [Vulnerabilidades](#) [Escaneo](#) [Ayuda](#)

**VULNERABILIDADES MÁS RECIENTES**

Nombre	Fecha de Publicación	Calificación	Gravedad	Opciones
CVE-2012-2682	19 de julio de 2014	5.0	Media	
CVE-2013-4273	19 de julio de 2014	4.0	Media	
CVE-2013-4352	20 de julio de 2014	4.3	Media	
CVE-2013-5567	14 de julio de 2014	5.4	Media	
CVE-2013-5755	16 de julio de 2014	7.8	Alta	
CVE-2013-5855	17 de julio de 2014	4.3	Media	
CVE-2013-6691	14 de julio de 2014	6.8	Media	
CVE-2013-7391	19 de julio de 2014	5.0	Media	
CVE-2013-7392	22 de julio de 2014	7.5	Alta	
CVE-2014-0117	20 de julio de 2014	4.3	Media	
CVE-2014-0118	20 de julio de 2014	4.3	Media	
CVE-2014-0226	20 de julio de 2014	6.8	Media	
CVE-2014-0231	20 de julio de 2014	5.0	Media	
CVE-2014-0436	17 de julio de 2014	4.3	Media	
CVE-2014-0957	17 de julio de 2014	4.3	Media	
CVE-2014-0967	19 de julio de 2014	3.5	Baja	
CVE-2014-0968	19 de julio de 2014	3.5	Baja	
CVE-2014-0970	19 de julio de 2014	3.5	Baja	
CVE-2014-1474	15 de julio de 2014	5.0	Media	
CVE-2014-1973	20 de julio de 2014	5.0	Media	

1 2 3 4 5 6 7 8 9 10 11 [Siguiente](#)

Figura 6 Tabla de Vulnerabilidades más recientes

Dentro de esta pantalla de cuenta con una tabla, la cual contiene:

- Nombre de la vulnerabilidad, de igual manera puede tomarse como identificador
- La fecha de publicación de la vulnerabilidad
- Su calificación y criticidad
- Enlace para visualización a detalle de la vulnerabilidad

Finalmente, en la parte inferior de la tabla se cuenta con un paginador que permite explorar entre las diversas vulnerabilidades presentadas.

Para explorar las vulnerabilidades presentadas, solo basta con elegir el número de página a consultar o hacer clic en el enlace 'Siguiente'.

Para conocer a detalle una vulnerabilidad, se tiene que elegir el botón que se encuentra al final de la fila de la vulnerabilidad deseada.

Una vez que se hizo clic en el icono, se debe mostrar la siguiente ventana:

Detalle de la Vulnerabilidad			
CVE-2012-2682			
Fecha de Publicación:	19 de julio de 2014		
Fecha de Modificación:	21 de julio de 2014		
Descripción:	Cumin (aka MRG Management Console), as used in Red Hat Enterprise MRG 2.5, allows attackers with certain database privileges to cause a denial of service (inaccessible page) via a non-ASCII character in the name of a link.		
Gravedad:	Media		
CVSS:	5.0		
Vector CVSS:	Vector Original	(AV:N/AC:L/Au:N/C:N/I:N/A:P)	
	Vector de Acceso:	Red	
	Complejidad de Acceso:	Baja	
	Autenticación:	No requerida	
	Impacto en Confidencialidad:	No tiene	
	Impacto en integridad:	No tiene	
	Impacto en Disponibilidad:	Parcial	
Referencias:	CONFIRM	<a href="https://bugzilla.redhat.com/show_bug.cgi?id=830254">https://bugzilla.redhat.com/show_bug.cgi?id=830254</a>	
	REDHAT	<a href="http://rhn.redhat.com/errata/RHSA-2014-0859.html">http://rhn.redhat.com/errata/RHSA-2014-0859.html</a>	
	REDHAT	<a href="http://rhn.redhat.com/errata/RHSA-2014-0858.html">http://rhn.redhat.com/errata/RHSA-2014-0858.html</a>	
Software Vulnerable:	Proveedor	Producto	Versión(es)
	REDHAT	enterprise_mrg	[2.5]
Descargar	<a href="#">Versión PDF</a>		

Figura 7 Detalle de una vulnerabilidad

En esta ventana, se muestra información más detallada de la vulnerabilidad como: descripción, vector de ataque, así como una lista de referencias y una lista de software vulnerable.

De igual manera, la ventana cuenta con un enlace con la descarga de la vulnerabilidad en formato PDF.

### Archivo de Vulnerabilidades

Para consultar el archivo de vulnerabilidades, hay que ubicar el apartado Vulnerabilidades de la barra de navegación y hacer clic sobre la opción 'Archivo' del menú desplegable.

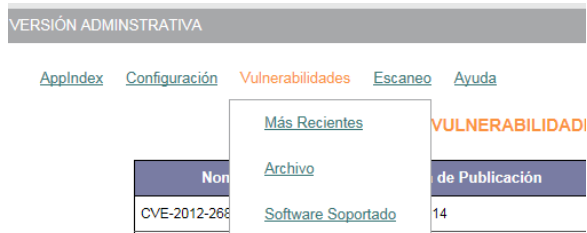



Figura 8 Menú desplegable de vulnerabilidades

Al seleccionar está opción se mostrara la siguiente pantalla:


**BANCO DE MÉXICO**

VERSIÓN ADMINISTRATIVA

[AppIndex](#)
[Configuración](#)
[Vulnerabilidades](#)
[Escaneo](#)
[Ayuda](#)

**ARCHIVO DE VULNERABILIDADES**

Nombre	Fecha de Publicación	Calificación	Gravedad	Opciones
CVE-2012-0001	10 de enero de 2012	9.3	Alta	
CVE-2012-0002	13 de marzo de 2012	9.3	Alta	
CVE-2012-0003	10 de enero de 2012	9.3	Alta	
CVE-2012-0004	10 de enero de 2012	9.3	Alta	
CVE-2012-0005	10 de enero de 2012	6.9	Media	
CVE-2012-0006	13 de marzo de 2012	5.0	Media	
CVE-2012-0007	10 de enero de 2012	4.3	Media	
CVE-2012-0008	13 de marzo de 2012	6.9	Media	
CVE-2012-0009	10 de enero de 2012	9.3	Alta	
CVE-2012-0010	14 de febrero de 2012	4.3	Media	
CVE-2012-0011	14 de febrero de 2012	9.3	Alta	
CVE-2012-0012	14 de febrero de 2012	4.3	Media	
CVE-2012-0013	10 de enero de 2012	9.3	Alta	
CVE-2012-0014	14 de febrero de 2012	9.3	Alta	
CVE-2012-0015	14 de febrero de 2012	9.3	Alta	
CVE-2012-0016	13 de marzo de 2012	9.3	Alta	
CVE-2012-0017	14 de febrero de 2012	4.3	Media	
CVE-2012-0018	8 de mayo de 2012	9.3	Alta	
CVE-2012-0019	14 de febrero de 2012	9.3	Alta	
CVE-2012-0020	14 de febrero de 2012	9.3	Alta	

Existen: 13116 vulnerabilidades.

Figura 9 Tabla de archivo de vulnerabilidades

Dentro de la pantalla se muestran los siguientes elementos:

- Barra de búsqueda de Vulnerabilidades
- Tabla de Vulnerabilidades
- Paginador

Para consultar el archivo, hay que seleccionar la opción Siguiente dentro del paginador que se encuentra en la sección inferior de la tabla de vulnerabilidades, para visualizar más detalle hay que hacer clic sobre el botón que se encuentra al final de la fila de la vulnerabilidad deseada.



Para buscar una vulnerabilidad hay que ingresar una de las siguientes opciones dentro del campo de búsqueda:

- Nombre o identificador completo de la vulnerabilidad
- Clave de la vulnerabilidad, que equivale a los últimos 4 o 5 dígitos de la vulnerabilidad

Figura 10 Barra de búsqueda

Una vez que se introdujo la clave a buscar, hay que dar clic en el botón Buscar, después se mostrará la siguiente pantalla con los resultados encontrados.

Nombre	Fecha de Publicación	Última Modificación	Calificación	Gravedad									
CVE-2014-0528	14-05-2014	14-05-2014	10.0	Alta									
Impacto:	Vector Original (AV:N/AC:L/Au:N/C:C/I:C/A:C) Vector de Acceso: Red Complejidad de Acceso: Baja Autenticación: No requerida Impacto en Confidencialidad: Completo Impacto en Integridad: Completo Impacto en Disponibilidad: Completo												
Descripción:	Double free vulnerability in Adobe Reader and Acrobat 10.x before 10.1.10 and 11.x before 11.0.07 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors.												
Software Vulnerable:	<table border="1"> <thead> <tr> <th>Fabricante</th> <th>Software</th> <th>Versión(es)</th> </tr> </thead> <tbody> <tr> <td>ADOBE</td> <td>ACROBAT</td> <td>[10.0, 10.0.1, 10.0.2, 10.0.3, 10.1, 10.1.1, 10.1.2, 10.1.3, 10.1.4, 10.1.5, 10.1.6, 10.1.7, 10.1.8, 10.1.9, 11.0, 11.0.1, 11.0.2, 11.0.3, 11.0.4, 11.0.5, edición: ~~~~windows~~~, 11.0.6]</td> </tr> <tr> <td>ADOBE</td> <td>ACROBAT_READER</td> <td>[10.0, 10.0.1, 10.0.2, 10.0.3, 10.1, 10.1.1, 10.1.2, 10.1.3, 10.1.4, 10.1.5, 10.1.6, 10.1.7, 10.1.8, 10.1.9, 11.0, 11.0.1, 11.0.2, 11.0.3, 11.0.4, 11.0.5, edición: ~~~~windows~~~, 11.0.6]</td> </tr> </tbody> </table>				Fabricante	Software	Versión(es)	ADOBE	ACROBAT	[10.0, 10.0.1, 10.0.2, 10.0.3, 10.1, 10.1.1, 10.1.2, 10.1.3, 10.1.4, 10.1.5, 10.1.6, 10.1.7, 10.1.8, 10.1.9, 11.0, 11.0.1, 11.0.2, 11.0.3, 11.0.4, 11.0.5, edición: ~~~~windows~~~, 11.0.6]	ADOBE	ACROBAT_READER	[10.0, 10.0.1, 10.0.2, 10.0.3, 10.1, 10.1.1, 10.1.2, 10.1.3, 10.1.4, 10.1.5, 10.1.6, 10.1.7, 10.1.8, 10.1.9, 11.0, 11.0.1, 11.0.2, 11.0.3, 11.0.4, 11.0.5, edición: ~~~~windows~~~, 11.0.6]
Fabricante	Software	Versión(es)											
ADOBE	ACROBAT	[10.0, 10.0.1, 10.0.2, 10.0.3, 10.1, 10.1.1, 10.1.2, 10.1.3, 10.1.4, 10.1.5, 10.1.6, 10.1.7, 10.1.8, 10.1.9, 11.0, 11.0.1, 11.0.2, 11.0.3, 11.0.4, 11.0.5, edición: ~~~~windows~~~, 11.0.6]											
ADOBE	ACROBAT_READER	[10.0, 10.0.1, 10.0.2, 10.0.3, 10.1, 10.1.1, 10.1.2, 10.1.3, 10.1.4, 10.1.5, 10.1.6, 10.1.7, 10.1.8, 10.1.9, 11.0, 11.0.1, 11.0.2, 11.0.3, 11.0.4, 11.0.5, edición: ~~~~windows~~~, 11.0.6]											
Referencias:	CONFIRM <a href="http://helpx.adobe.com/security/products/reader/apsb14-15.html">http://helpx.adobe.com/security/products/reader/apsb14-15.html</a>												

Figura 11 Resultados de la búsqueda

Finalmente, para terminar la búsqueda se tiene que hacer clic en el botón Terminar búsqueda.

## Software Soportado

La aplicación permite conocer el software que se tiene registrado en la base de datos, sobre estos elementos es sobre los que se hace el análisis para buscar vulnerabilidades.

Para consultar estos elementos, se tiene que ubicar el apartado Vulnerabilidades y seleccionar la opción 'Software Soportado' dentro del menú desplegable.



Figura 12 Menú desplegable de vulnerabilidades

Una vez hecho esto se desplegará la siguiente pantalla:

SOFTWARE SOPORTADO

+ Agregar Software

Nombre del SW o de Grupo

Fabricante	Software	Version	Grupo
SweetScape Software Inc.	010 Editor 2.x	2.x	sw-Huerfano
Adobe Systems	Adobe Acrobat 6.x	6.x	Windows XP
Adobe Systems	Adobe Acrobat 7.x	7.x	Windows XP
Adobe Systems	Adobe Acrobat 7.x	7.x	SW_top20
Adobe Systems	Adobe Acrobat 8.x	8.x	DGTI
Adobe Systems	Adobe Acrobat 8.x	8.x	SW_top20
Adobe Systems	Adobe Acrobat 9.x	9.x	DGTI
Adobe Systems	Adobe Acrobat 9.x	9.x	SW_top20
Adobe Systems	Adobe Acrobat X 10.x	10.x	sw-Huerfano
Adobe Systems	Adobe Digital Editions 1.x	1.x	ETB
Adobe Systems	Adobe Flash Builder 4.x	4.x	sw-Huerfano
Adobe Systems	Adobe Flash Player 10.x	10.x	DGTI
Adobe Systems	Adobe Flash Player 10.x	10.x	SW_top20
Adobe Systems	Adobe Flash Player 11.x	11.x	ETB
Adobe Systems	Adobe Flash Player 11.x	11.x	SW_top20
Adobe Systems	Adobe Flash Player 12.x	12.x	SW_top20
Adobe Systems	Adobe Flash Player 13.x	13.x	SW_top20
Adobe Systems	Adobe Flash Player 14.x	14.x	SW_top20
Adobe Systems	Adobe Flash Player 9.x	9.x	ETB
Adobe Systems	Adobe Flash Player 9.x	9.x	SW_top20

1

Figura 13 Tabla de software soportado

La pantalla cuenta con los siguientes elementos:

- Barra de búsqueda de software
- Tabla de software soportado
- Paginador

Para realizar una búsqueda de software, se tiene que ingresar el nombre del software o el nombre del grupo dentro del campo de búsqueda, una vez ingresado, hacer clic en el botón buscar.

Figura 14 Barra de búsqueda de software

Los resultados serán mostrados en una tabla, como la que se muestra en la siguiente pantalla:

Fabricante	Software	Versión	Grupo
Sybase	Sybase Adaptive Server Enterprise 15.x	15.x	AIX 6x
Sybase	Sybase Adaptive Server Enterprise 12.x	12.x	AIX 6x
Sendmail Consortium	Sendmail 8.x	8.x	AIX 6x
Oracle Corporation	Oracle9i Database Enterprise Edition	9i	AIX 6x
Oracle Corporation	Oracle9i Database Standard Edition	9i	AIX 6x
Oracle Corporation	Oracle9i Application Server	9i	AIX 6x
Oracle Corporation	Oracle Java SDK 1.4.x/4.x	1.4.x	AIX 6x
Oracle Corporation	Oracle HTTP Server 10.x	10.x	AIX 6x
Oracle Corporation	Oracle Enterprise Manager 11.x	11.x	AIX 6x
Oracle Corporation	Oracle Enterprise Manager 10.x	10.x	AIX 6x
OpenSSL	OpenSSL 0.x	0.x	AIX 6x
OpenBSD	OpenSSH 5.x	5.x	AIX 6x
IBM	IBM Java 1.4.x	1.4.x	AIX 6x
IBM	Aix 6.x	6.x	AIX 6x

Figura 15 Resultados de búsqueda de software

## Escaneo

Para buscar vulnerabilidad dentro del inventario, hay que seleccionar la opción 'Escaneo' que se encuentra en la barra de navegación de la aplicación. Al hacer clic se mostrara la siguiente pantalla:



NUEVO ESCANEO

[ApplIndex](#) [Configuración](#) [Vulnerabilidades](#) [Escaneo](#) [Ayuda](#)

**REALIZAR ESCANEO**

Tipo de Escaneo:

☐ Completo

☐ Personalizado

*Figura 16 Pantalla de Escaneo*

El escaneo se puede realizar de 2 maneras:

- Completo

En este tipo de escaneo se realizara una comparación de todos los elementos del inventario con todo el archivo de vulnerabilidades. Se puede realizar en todo el periodo de tiempo registrado o desde un tiempo especificado por el usuario.

- Personalizado

Aquí se puede realizar un escaneo a partir de un grupo específico, un fabricante específico, periodos de tiempo específicos y realizar búsquedas en fechas de publicación o modificación o ambas.

Para configurar un escaneo completo, se debe elegir la opción 'Completo' en la pantalla anteriormente mostrada, al seleccionar esta opción se mostrara un nuevo campo en el cual se puede hacer la selección del tiempo para realizar el escaneo.

**BANCO DE MÉXICO**

NUEVO ESCANEO

[ApplIndex](#) [Configuración](#) [Vulnerabilidades](#) [Escaneeo](#) [Ayuda](#)

**REALIZAR ESCANEO**

Tipo de Escaneo: ☒ Completo ☐ Personalizado

Esté escaneo analizará (todos los grupos/todas las UA) con el archivo completo de Vulnerabilidades.

Seleccionar periodo de escaneo:

Periodo ☐ Completo ☒ Específico

Fecha de Inicio: 15/06/2014

Fecha de Fin:

Calendar: Jul 2014

Lu	Ma	Mi	Ju	Vi	Sá	Do
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

Figura 17 Selección de fechas de escaneo

Una vez seleccionadas las fechas, se debe hacer clic sobre el botón 'Escanear', el cual se encargará de solicitar los resultados conforme a los parámetros establecidos.

**BANCO DE MÉXICO**

NUEVO ESCANEO

[ApplIndex](#) [Configuración](#) [Vulnerabilidades](#) [Escaneeo](#) [Ayuda](#)

**REALIZAR ESCANEO**

Tipo de Escaneo: ☒ Completo ☐ Personalizado

Esté escaneo analizará (todos los grupos/todas las UA) con el archivo completo de Vulnerabilidades.

Seleccionar periodo de escaneo:

Periodo ☐ Completo ☒ Específico

Fecha de Inicio: 01/07/2014

Fecha de Fin: 23/07/2014

**Escanear**

Figura 18 Botón de Escaneo

Una vez realizado el escaneo, se listan los resultados, mostrando información como:

- El nombre de la vulnerabilidad
- El software que puede ser afectado
- La gravedad de la vulnerabilidad y
- Los grupos que pueden ser afectados por la vulnerabilidad.

Los resultados son mostrados en forma tabular para facilitar su lectura.


 BANCO DE MÉXICO				
VERSIÓN ADMINISTRATIVA				
<a href="#">Configuración</a> <a href="#">Vulnerabilidades</a> <a href="#">Escaneo</a> <a href="#">Ayuda</a>				
SE ENCONTRARON: 36 POSIBLES AMENAZAS.				
Vulnerabilidad	Software Afectado	Gravedad	Fecha de Publicación	Grupos Afectados
CVE-2014-0207	PHP 5.4.x PHP 5.5.x	Media	9 de julio de 2014	SW_top20
The cdf_read_short_sector function in cdf.c in file before 5.19, as used in the Fileinfo component in PHP before 5.4.30 and 5.5.x before 5.5.14, allows remote attackers to cause a denial of service (assertion failure and application exit) via a crafted CDF file.				
CVE-2014-0537	Adobe Flash Player 11.x Adobe Flash Player 13.x Adobe Flash Player 14.x	Alta	9 de julio de 2014	ETB SW_top20
Adobe Flash Player before 13.0.0.231 and 14.x before 14.0.0.145 on Windows and OS X and before 11.2.202.394 on Linux, Adobe AIR before 14.0.0.137 on Android, Adobe AIR SDK before 14.0.0.137, and Adobe AIR SDK				
CVE-2014-0539	Adobe Flash Player 11.x Adobe Flash Player 13.x Adobe Flash Player 14.x	Alta	9 de julio de 2014	ETB SW_top20
Adobe Flash Player before 13.0.0.231 and 14.x before 14.0.0.145 on Windows and OS X and before 11.2.202.394 on Linux, Adobe AIR before 14.0.0.137 on Android, Adobe AIR SDK before 14.0.0.137, and Adobe AIR SDK				
CVE-2014-1767	Microsoft Windows 7 Microsoft Windows 7 Embedded Microsoft Windows 8 Microsoft Windows 8.1 Microsoft Windows Server 2003 Enterprise Edition Microsoft Windows Server 2003 Standard Edition Microsoft Windows Server 2008 Microsoft Windows Server 2012	Alta	8 de julio de 2014	SW Red Interna SW Telefonía Windows 7 Windows XP Microsoft Windows Server 2003 Enterprise Edition Microsoft Windows Server XXXX OASR Servidores OSI Trend Websense consola OASR NEW OS

Figura 19 Resultados del escaneo

Los resultados pueden ser exportados en formato de texto, para facilitar la manipulación de los mismos por parte del personal de la OSI.

Para realizar la exportación basta con hacer clic sobre el botón 'Versión Texto' que se encuentra ubicado en la parte inferior de la tabla de resultados.

CVE-2014-4721	PHP 5.3.x PHP 5.4.x PHP 5.5.x PHPX 3.x	Baja	6 de julio de 2014	SW_top20
<p>The phinfo implementation in ext/standard/info.c in PHP before 5.4.30 and 5.5.x before 5.5.14 does not ensure use of the string data type for the PHP_AUTH_PW, PHP_AUTH_TYPE, PHP_AUTH_USER, and PHP_SELF variables, which might allow context-dependent attackers to obtain sensitive information from process memory by using the integer data type with crafted values, related to a "type confusion" vulnerability, as demonstrated by reading a private SSL key in an Apache HTTP Server web-hosting environment with mod_ssl and a PHP 5.3.x mod_php.</p>				
<div>Versión Texto</div>				

Figura 20 Botón de exportación

Al hacer esto se mostrara una ventana con el contenido representado en forma de texto, tal como se muestra en la siguiente ventana:

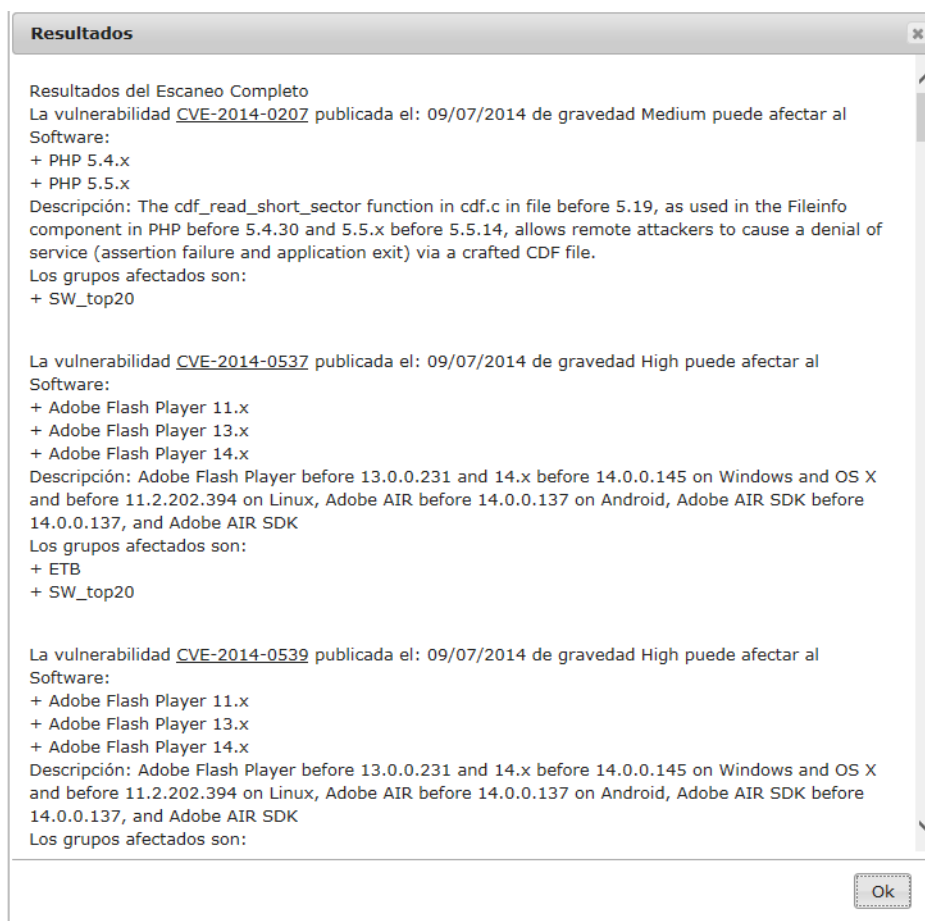


Figura 21 Resultados en formato de texto