

CVE-alert

Rafael Otal - Jorge Puente
Sistemas de Información
Mayo 2018





¿Quienes somos?

- 3000 alumnos
- 26 carreras
- 20 Posgrados y especializaciones
- 3 Doctorados
- 13 años



Jorge Puente

- Ing. Informática
- Programador - USJ
- Especializado en CMS



@forges82

Rafael Ota

- Ing. Técnico en Telecomunicaciones
- Co-Creador de AdminServer - Securipy
- IT Security Auditor
- Organizador MorterueloCon, HB
- Clso USJ



@goldrak

Índice

- Vul... que¿?
- Y eso se mide?
- Mis usuarios y su software
- GLPI
- CVE-alert

Vul... que?!

Las vulnerabilidades de un sistema son una puerta abierta para posibles ataques, de ahí que sea tan importante tenerlas en cuenta; en cualquier momento podrían ser aprovechadas.





Y eso se mide?

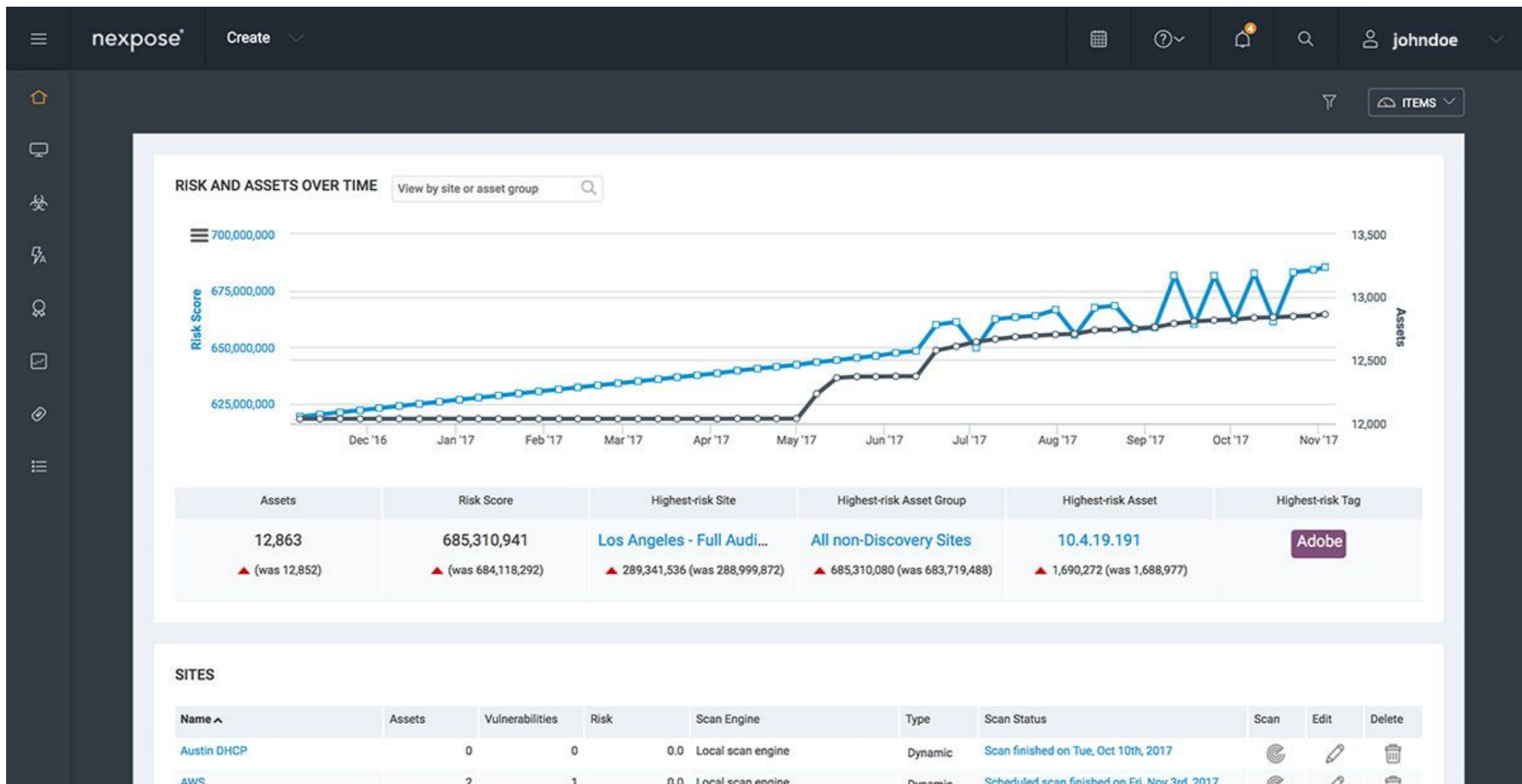
- CVE
- EDB-ID
- BID
- Medidas propias
-



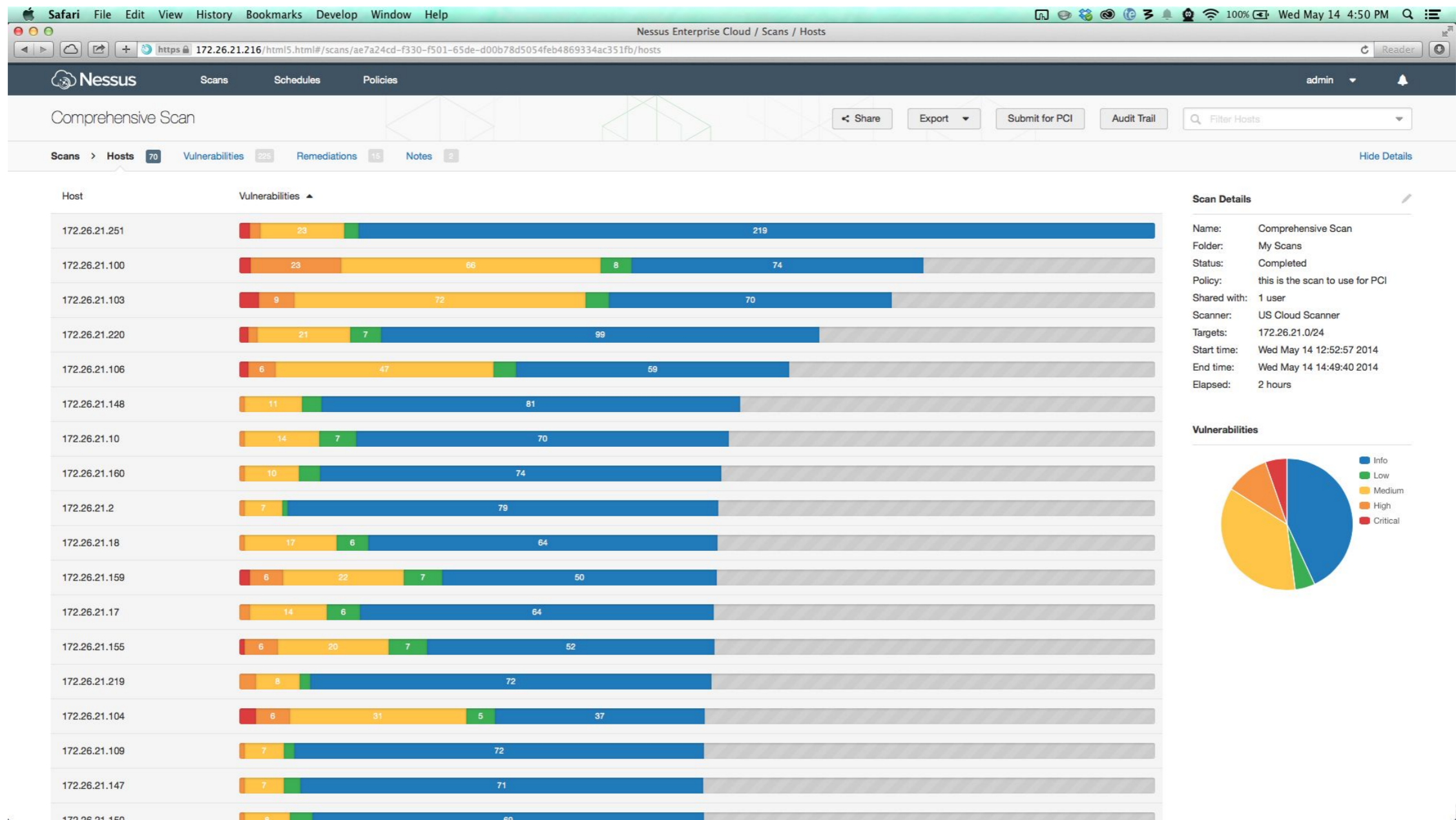
Mis usuarios y su software



Mis usuarios y su software



Mis usuarios y su software





Mis usuarios y su software

Network inventory advisor

Inventory Reports

Wizard New asset Export audit agent Import nodes Manage your network

Manage nodes Rename selected asset Manage networks

Scan my PC only Scan selected Scan other PC Scan network

Schedule scanning Network summary Search report Report

Update report now All network alerts

Export this now Print Settings Options

Network structure

ABC Network

Network summary (130)

- Collocation (3)
 - PC0132
 - PC0133
 - PC0134
- Devices (15)
 - PC0010
 - PC0011
 - PC0012
 - PC0013
 - PC0014
 - PC0015
 - PC0016
 - PC0017
 - PC0018
 - PC0019
 - PC0020
 - PC0021
 - PC0022
 - PC0023
 - PC0024
- Linux Systems (2)
 - PC0135
 - PC0136
- PData Servers (9)

Network summaries: **YESTERDAY** Monday, November 26, 2012, 11:55:44 PM Monday, November 26, 2012, 11:53:51 PM ...see all

All soft Search Show hidden Group Mark as

Display Manage

Software title	V.	Publisher	Fo...	L	Delta
Microsoft Office 2007		Microsoft	98	99	1
2007 Microsoft Office Suite Servi...		Microsoft	1	see i...	0
2007 Microsoft Office system	12	Microsoft Corpor...	29	see i...	0
Activation Assistant for the 2007 ...		Microsoft Corpor...	1	see i...	0
Microsoft Office 2007 Primary Inte...	12	Microsoft Corpor...	1	see i...	0
Microsoft Office 2007 Service Pa...		Microsoft	24	see i...	0
Microsoft Office Access 2007	12	Microsoft Corpor...	1	see i...	0
Microsoft Office Live Meeting 2007	8	Microsoft Corpor...	1	see i...	0
Microsoft Office PowerPoint 2007	12	Microsoft Corpor...	3	see i...	0
Microsoft Office PowerPoint View...	12	Microsoft Corpor...	5	see i...	0
Microsoft Office Professional Plus...	12	Microsoft Corpor...	3	see i...	0
Microsoft Office Standard 2007	12	Microsoft Corpor...	1	see i...	0
Microsoft Office Visio 2007 Servic...		Microsoft	2	see i...	0
Microsoft Office Visio Standard 2...	12	Microsoft Corpor...	3	see i...	0
Security Update for Microsoft Off...		Microsoft	23	see i...	0
Microsoft Office 2010		Microsoft	0	not ...	0
Microsoft Office Live Add-in 1.4	2	Microsoft Corpor...	1	not set	0
Microsoft Office Professional Plus 20...	15	Microsoft Corpor...	1	not set	0
Microsoft Office Proofing Tools 2013 ...	15	Microsoft Corpor...	1	not set	0
Microsoft Office Small Business Conn...	2	Microsoft Corpor...	1	not set	0

Network summary

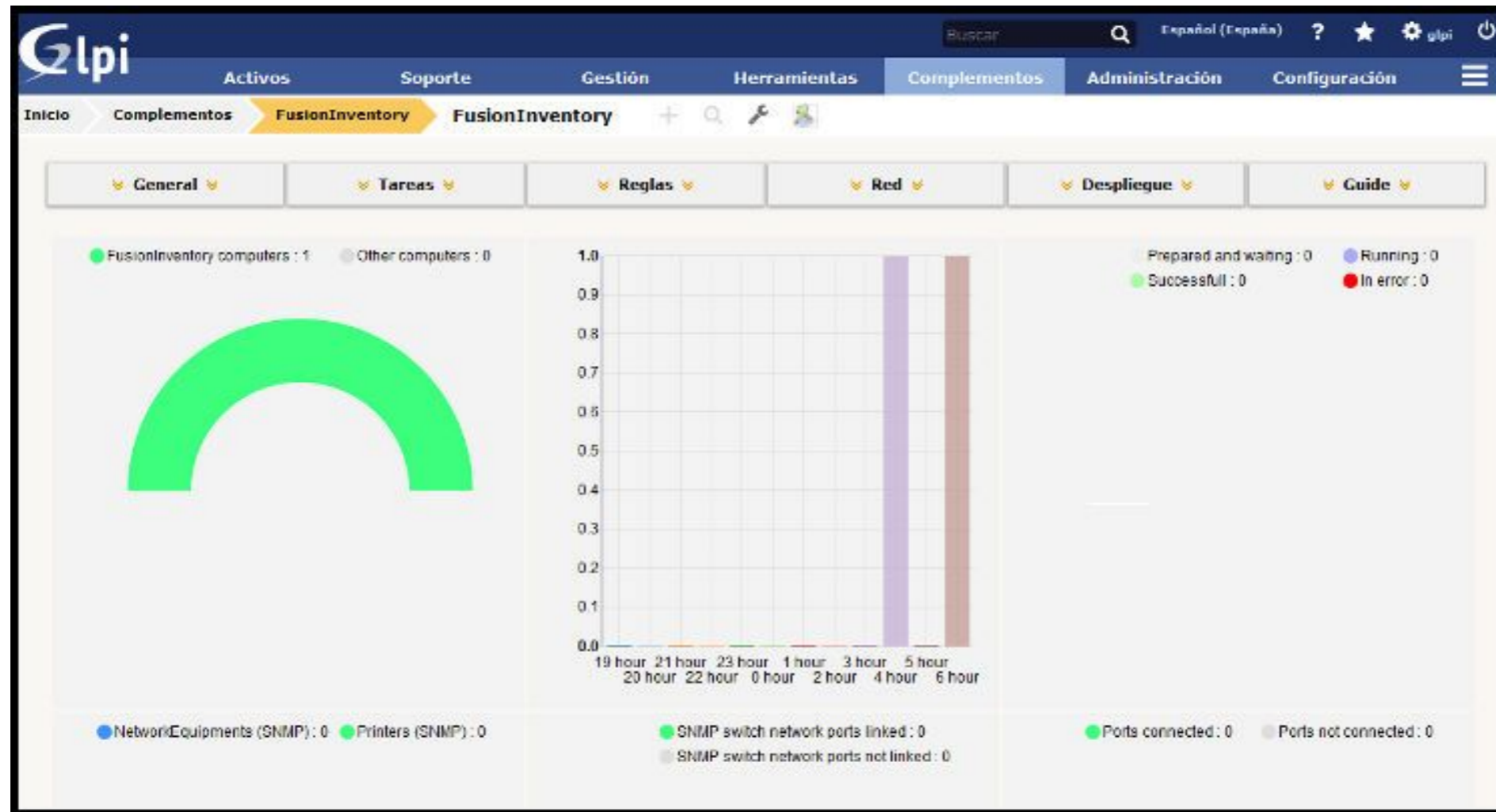
- All software
- All license keys
- All hardware
- All alerts

Scan log

Using NationWide license. 273 nodes managed in all networks. => more nodes can still be added.

Navigation

Mis usuarios y su software



Mis usuarios y su software

Show: 20


Restrict view: Filter X

Add column: X


67 Result(s) (Download)

Account info: Etiqueta X	Last inventory X	Computer	User X	Operating system X	RAM (MB) X	CPU (MHz) X	Select	Delete
ORD-DINF-A23-02	2013-05-31 11:40:15	ORD-DINF-A23-02	alum-01	Microsoft Windows 7 Professional	4096	2600	<input type="checkbox"/>	X
Sense etiqueta	2013-05-31 09:29:12	PEDRO-PC	Pedro	Microsoft Windows 7 Ultimate	4096	2600	<input type="checkbox"/>	X
ORD-DINF-A23-03	2013-05-31 07:11:13	ORD-DINF-A23-03	ruben	Ubuntu 12.04.1 LTS	3854	2100	<input type="checkbox"/>	X
ORD-DINF-A22-03	2013-05-31 07:10:45	ORD-DINF-A22-01	profe	Microsoft Windows 7 Professional	2048	2693	<input type="checkbox"/>	X
ORD-DINF-A24-PF	2013-05-31 06:27:19	ORD-DINF-A24-PF	profe	Microsoft Windows 7 Professional	2048	2700	<input type="checkbox"/>	X
ORD-DINF-A22-10	2013-05-31 06:11:58	SINTESIS-PC	Sintesis	Microsoft Windows 7 Ultimate	3489	3001	<input type="checkbox"/>	X
Sense etiqueta	2013-05-30 16:41:28	DEPARTAMENT-JAV	alumne	Microsoft Windows 7 Professional	3327	2712	<input type="checkbox"/>	X
Sense etiqueta	2013-05-30 06:47:30	ALUMNE-PC2	alumne	Microsoft Windows 7 Professional	3489	3001	<input type="checkbox"/>	X
ORD-DINF-A22-01	2013-05-30 06:40:45	ALUMNE-PC1	alumne	Microsoft Windows 7 Professional	3489	3001	<input type="checkbox"/>	X
ORD-DINF-A22-08	2013-05-30 06:27:52	ALUMNE-PC	alumne	Microsoft Windows 7 Professional	3489	3001	<input type="checkbox"/>	X
Sense etiqueta	2013-05-29 07:00:50	CARLOS-B	alumne	Microsoft Windows 7 Professional	2048	2700	<input type="checkbox"/>	X
ORD-DINF-A22-17	2013-05-29 06:29:50	SERGI-PC	alumne	Microsoft Windows 7 Professional	3489	3001	<input type="checkbox"/>	X
ORD-DINF-A24-01	2013-05-24 11:48:55	ord-dinf-au24-01	profe	Ubuntu 12.04.1 LTS	1884	1203	<input type="checkbox"/>	X
ORD-DINF-A24-11	2013-05-23 07:36:31	ORD-DINF-A24-11	ubuntu	Ubuntu 12.04.1 LTS	1968	2700	<input type="checkbox"/>	X
ORD-DINF-A24-09	2013-05-23 07:35:02	ORD-DINF-A24-09	ubuntu	Ubuntu 12.04.1 LTS	1968	2700	<input type="checkbox"/>	X
ORD-DINF-A24-14	2013-05-23 07:14:22	ORD-DINF-A24-14	ubuntu	Ubuntu 12.04.1 LTS	1936	1203	<input type="checkbox"/>	X
ORD-DINF-A24-15	2013-05-23 07:01:54	ORD-DINF-A24-15	ubuntu	Ubuntu 12.04.1 LTS	1968	2700	<input type="checkbox"/>	X
ORD-DINF-A24-17	2013-05-23 06:43:46	ORD-DINF-A24-17	ubuntu	Ubuntu 12.04.1 LTS	1968	1203	<input type="checkbox"/>	X
ORD-DINF-A23-02	2013-05-22 06:40:50	ORD-DINF-A23-02	alum-01	Microsoft Windows 7 Professional	4096	2600	<input type="checkbox"/>	X
ORD-DINF-A24-16	2013-05-22 06:36:00	ORD-DINF-A24-16	ubuntu	Ubuntu 12.04.1 LTS	1968	1203	<input type="checkbox"/>	X

0 1 2 3 >>>



102.169.123.149/.../index.php?function=computer&board=1&usuarioid=90




Mis usuarios y su software

Plugin's features

Replace ticket's items association Show prelude alerts in tickets

API Access

Prelude URL 

API Client ID

API Client Secret

API Access token [Connect to Prelude API](#)

API Status


Prelude	<input checked="" type="checkbox"/>
Prelude access token	<input type="checkbox"/>
Prelude alerts	<input type="checkbox"/>
Prelude logs	<input type="checkbox"/>

GLPI

universidad **SANJORGE** GRUPO SANVALERO

Activos Soporte Gestión Herramientas Complementos Administración Configuración


Inicio super-admin




Abierto

0


Nuevo



En curso



Cerrado








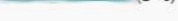
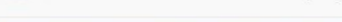
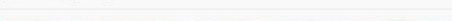
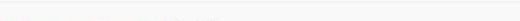
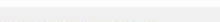
En espera

0

Atrasado

Vista personal Vista de grupo Vista global Canales RSS Todos

Sus peticiones en curso 10

ID	Solicitante	Elementos asociados	Descripción
ID: 28746	OTAL SIMAL RAFAEL i	General	 (1 - 0)
ID: 28730	OTAL SIMAL RAFAEL i	General	 04 (1 - 0)
ID: 28693	OTAL SIMAL RAFAEL i	General	 (0 - 0)
ID: 28666	OTAL SIMAL RAFAEL i	General	 (0 - 0)
ID: 28669	OTAL SIMAL RAFAEL i	General	 (2 - 0)
ID: 28657	OTAL SIMAL RAFAEL i	General	 (1 - 0)
ID: 28668	OTAL SIMAL RAFAEL i	General	 (1 - 0)
ID: 28663	OTAL SIMAL RAFAEL i	General	 (1 - 0)
ID: 28664	OTAL SIMAL RAFAEL i	General	 2 (2 - 0)
ID: 28063	OTAL SIMAL RAFAEL i	General	 (1 - 0)



Su planificación

No hay eventos para mostrar

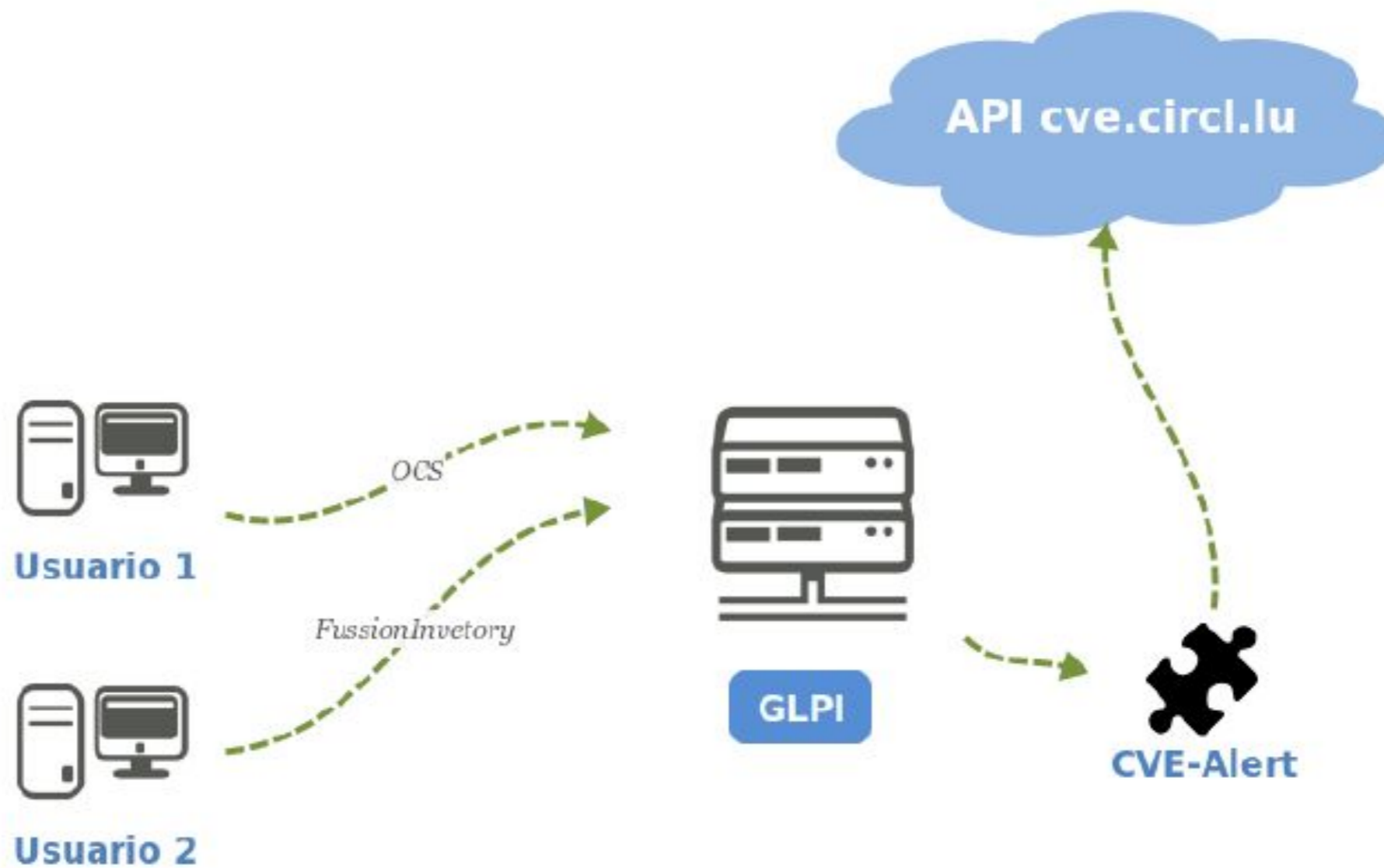
Recordatorios personales +

Recordatorios públicos +

Sus peticiones observadas 2

ID	Solicitante	Elementos asociados	Descripción
ID: 28663	OTAL SIMAL RAFAEL i	General	 (1 - 0)
ID: 28664	OTAL SIMAL RAFAEL i	General	 2 (2 - 0)

CVE-Alert



CVE-Alert



universidad **SANJORGE** GRUPO SANVALERO

17 0 0 Buscar ? ★ ⚙️ PUENTE GARCIA JORGE



Activos Soporte Gestión Herramientas Complementos Administración Configuración

Inicio Complementos **CVE Alert** + 🔍 super-admin


Elementos mostrados contiene Buscar ★ ⌂

Muestra (número de elementos) 20  Página actual en PDF apaisado  Desde 1 hasta 2 de 2

Acciones

<input type="checkbox"/>	- Software	- Name manufacturer	- Name software	- Enlace software
<input type="checkbox"/>	ADOBE ACROBAT PRO 9	adobe	acrobat_business_tools	
<input type="checkbox"/>	ADOBE DREAMWEAVER	adobe	dreamweaver_cs3	

Acciones

Muestra (número de elementos) 20  Desde 1 hasta 2 de 2

CVE-Alert

universidad **SANJORGE** GRUPO SANVALERO

17 0 0 Buscar ? ★ ⚙️ PUENTE GARCIA JORGE

Activos Soporte Gestión Herramientas Complementos Administración Configuración

Inicio Complementos CVE Alert + 🔍 super-admin

Equivalencia CVE Alert

Nuevo elemento - Equivalencia CVE Alert

Software ⓘ

CVE Manufacturer

CVE Software

Selecciona un Manufacturer

Añadir

CVE-Alert

universidad
SANJORGE
GRUPO SANVALERO

Activos Soporte Gestión Herramientas Complementos Administración Configuración

Inicio Complementos **CVE Alert** + Q

super-admin

Equivalencia CVE Alert

Nuevo elemento - Equivalencia CVE Alert

Software

CVE Manufacturer

CVE Software

ADOBE ACROBAT PRO 9

Entidad raíz

- ADOBE ACROBAT PRO 9
- ADOBE ACROBAT PRO 9 EXTENDED
- ADOBE AUDITION
- ADOBE CREATIVE SUITE DESIGN PREMIUM
- ADOBE DREAMWEAVER
- ADOBE FREEHAND
- ADOBE INDESIGN
- AVID MEDIA COMPOSER 4.0

0.145 segundos - 8.08 MB

Copyright (C) 2015-2017 Teclib' and contributors - Copyright (C) 2003-2015 INDEPNET Development Team

CVE-Alert

universidad **SANJORGE** GRUPO SANVALERO

Activos Soporte Gestión Herramientas Complementos Administración Configuración

Inicio Complementos **CVE Alert** + Q

super-admin

Equivalencia CVE Alert

Nuevo elemento - Equivalencia CVE Alert

Software	ADOBE DREAMWEAVER
CVE Manufacturer	adobe
CVE Software	acrobat

- drea
- dreamweaver**
- dreamweaver_cs3
- dreamweaver_cs4
- dreamweaver_cs5.5
- dreamweaver_mx

0.145 segundos - 8.08 MB

GLPI 9.2.1 Copyright (C) 2015-2017 Teclib' and contributors - Copyright (C) 2003-2015 INDEPNET Development Team

CVE-Alert

universidad
SANJORGE
GRUPO SANVALERO

17 0 0 Buscar ? ★ ⚙️ PUENTE GARCIA JORGE

Activos Soporte Gestión Herramientas Complementos Administración Configuración

Inicio Complementos **CVE Alert** + 🔍 super-admin

« < Lista... **Equivalencia CVE Alert - adobe acrobat_business_tools** 1/3 > »

Equivalencia CVE Alert

Software	ADOBE ACROBAT PRO 9 ⓘ
CVE Manufacturer	adobe
CVE Software	acrobat_business_tools

Actualizar Delete

0.144 segundos - 8.08 MB

GLPI 9.2.1 Copyright (C) 2015-2017 Teclib' and contributors - Copyright (C) 2003-2015 INDEPNET Development Team

CVE-Alert

universidad **SANJORGE** GRUPO SANVALERO

Activos Soporte Gestión Herramientas Complementos Administración Configuración

Inicio Activos Computadores + Q ☰

super-admin

Lista... **Computador - HP 6710**

Computador

Sistemas operativos 1

Componentes

Volúmenes

Software 2

Conexiones

Puertos de red

Gestión

Software

Muestra (número de elementos) 20 Desde 1 hasta 2 de 2

Nombre	Versión	Fabricante	CVE
ADOBE ACROBAT PRO 9	9	ADOBE	Q
ADOBE INDESIGN	CS4	ADOBE	+

Nombre	Versión	Fabricante	CVE
--------	---------	------------	-----

CVE-Alert

The screenshot shows a web interface for CVE-Alert. The top navigation bar includes the university logo, a search bar, and user information (PUENTE GARCIA JORGE). The main navigation menu has tabs for Activos, Soporte, Gestión, Herramientas, Complementos, Administración, and Configuración. The current view is 'Activos' > 'Computadores'. A modal window titled 'Posibles vulnerabilidades' is open, displaying a table with the following data:

Fecha de publicación	Score	CVE	Link
2000-10-20	7.6	CVE-2000-0713	🔗

Below the modal, a table shows the manufacturer and CVE details for the vulnerability:

Fabricante	CVE
ADOBE	Q
ADOBE	+
Fabricante	CVE

CVE-Alert

CVE Details

The ultimate security vulnerability datasource

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

 Search

 View CVE

[Log In](#) [Register](#)

Vulnerability Feeds & WidgetsNew www.itsecdb.com

[Switch to https://](#)

[Home](#)

Browse :

[Vendors](#)

[Products](#)

[Vulnerabilities By Date](#)

[Vulnerabilities By Type](#)

Reports :

[CVSS Score Report](#)

[CVSS Score Distribution](#)

Search :

[Vendor Search](#)

[Product Search](#)

[Version Search](#)

[Vulnerability Search](#)

[By Microsoft References](#)

Top 50 :

[Vendors](#)

[Vendor Cvss Scores](#)

[Products](#)

[Product Cvss Scores](#)

[Versions](#)

Other :

[Microsoft Bulletins](#)

[Bugtraq Entries](#)

[CWE Definitions](#)

[About & Contact](#)

[Feedback](#)

Vulnerability Details : [CVE-2000-0713](#)

Buffer overflow in Adobe Acrobat 4.05, Reader, Business Tools, and Fill In products that handle PDF files allows attackers to execute arbitrary commands via a long /Registry or /Ordering specifier.

Publish Date : 2000-10-20 Last Update Date : 2008-09-05

[Collapse All](#) [Expand All](#) [Select](#) [Select&Copy](#) [Scroll To](#) [Comments](#) [External Links](#)

[Search Twitter](#) [Search YouTube](#) [Search Google](#)

- CVSS Scores & Vulnerability Types

CVSS Score	7.6
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	High (Specialized access conditions exist. It is hard to exploit and several special conditions must be satisfied to exploit)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	Admin
Vulnerability Type(s)	Execute Code Overflow
CWE ID	CWE id is not defined for this vulnerability

- Products Affected By CVE-2000-0713

#	Product Type	Vendor	Product	Version	Update	Edition	Language
---	--------------	--------	---------	---------	--------	---------	----------

CVE-Alert

- V1 - Beta 1
 - Agregar correlación de datos.
 - Consulta del software con la base de datos de CVE.
- V1 - Beta 2
 - Envío automático de email.
 - Listado de ordenadores con el software instalado.
 - Generación de informes de vulnerabilidades.
 - Configuración de base de datos propia.
- V1
 - Panel central con información del estado.
 - alguna ocurrencia que aportéis.



www.usj.es

Gracias a todos