

# Seguridad y Alta Disponibilidad: Introducción (II)



IES Gonzalo Nazareno  
**CONSEJERÍA DE EDUCACIÓN**

Jesús Moreno León

jesus.moreno.edu@  
juntadeandalucía.es

Septiembre 2012


---

Estas diapositivas son una obra derivada de los seminarios de formación impartidos por **Marta Beltrán** y **Antonio Guzman** de la URJC

© Jesús Moreno León, Septiembre de 2012

Algunos derechos reservados.  
Este artículo se distribuye bajo la licencia  
"Reconocimiento-CompartirIgual 3.0 España" de Creative  
Commons, disponible en  
<http://creativecommons.org/licenses/by-sa/3.0/es/deed.es>

Este documento (o uno muy similar)  
está disponible en (o enlazado desde)  
<http://informatica.gonzalonazareno.org>



## Algo de terminología

---

- **Activos:** elementos que pertenecen a la empresa y que se quieren proteger
  - Datos
  - Software
  - Hardware
  - Instalaciones
  - Personal
  - Servicios
- **Amenazas:**
  - Interrupción
  - Interceptación
  - Modificación
  - Fabricación



# Algo de terminología

- **Vulnerabilidad:** es un fallo en el diseño o configuración de un software

Una vulnerabilidad genera un expediente de seguridad identificado por su CVE (Common Vulnerabilities and Exposures)

<http://secunia.com/advisories/>

## Advisories

The archives page allows you to get a quick overview of all Secunia advisories and vulnerabilities released. Secunia advisories cover vulnerabilities announced for all types of programs and operating systems.

Secunia continuously updates advisories to reflect new data whenever it becomes available. **On average Secunia releases between 15 and 20 new advisories and updates more than 20 Secunia advisories on a daily basis.**

Track vulnerabilities with our Vulnerability Intelligence solution [VIM](#) for instant alerts and filtered vulnerability information.

19th Sep, 2012

[Cisco IOS SSLVPN Denial of Service Vulnerability](#) **New**

102 views



[WordPress Answer My Question Plugin "user\\_name" and "subject" Script Insertion Vulnerabilities](#) **New**

93 views



[osCommerce Website Payments Standard Module Merchant Email Address Security Bypass](#) **New**

84 views



[WordPress Purity Theme Multiple Cross-Site Scripting Vulnerabilities](#) **New**

89 views



[Cisco Nexus 7000 Series NX-OS ARP Packet Handling Denial of Service](#)

145 views



[Cisco Identity Services Engine Cross-Site Request Forgery](#)

130 views



[LuxCal Web Calendar Multiple Vulnerabilities](#)

79 views



[Ubuntu update for isc-dhcp and dhcp3](#)

118 views



[SUSE update for otrs](#)

105 views



[SUSE update for chromium](#)

113 views



[Red Hat update for java-1.7.0-ibm](#)

139 views



[Red Hat update for libxml2](#)

151 views



## Latest advisories

New advisories: 22  
New vulnerabilities: 63  
Updated advisories: 62

102 views  
[Cisco IOS SSLVPN Denial of Service Vulnerability](#) **New**

93 views  
[WordPress Answer My Question Plugin "user\\_name" and "subject" Script Insertion Vulnerabilities](#) **New**

84 views  
[osCommerce Website Payments Standard Module Merchant Email Address Security Bypass](#) **New**

89 views  
[WordPress Purity Theme Multiple Cross-Site Scripting Vulnerabilities](#) **New**

## Algo de terminología

---

- Tiempos de reacción y día cero

Se define como **día cero**, el día en el que se hace pública una vulnerabilidad

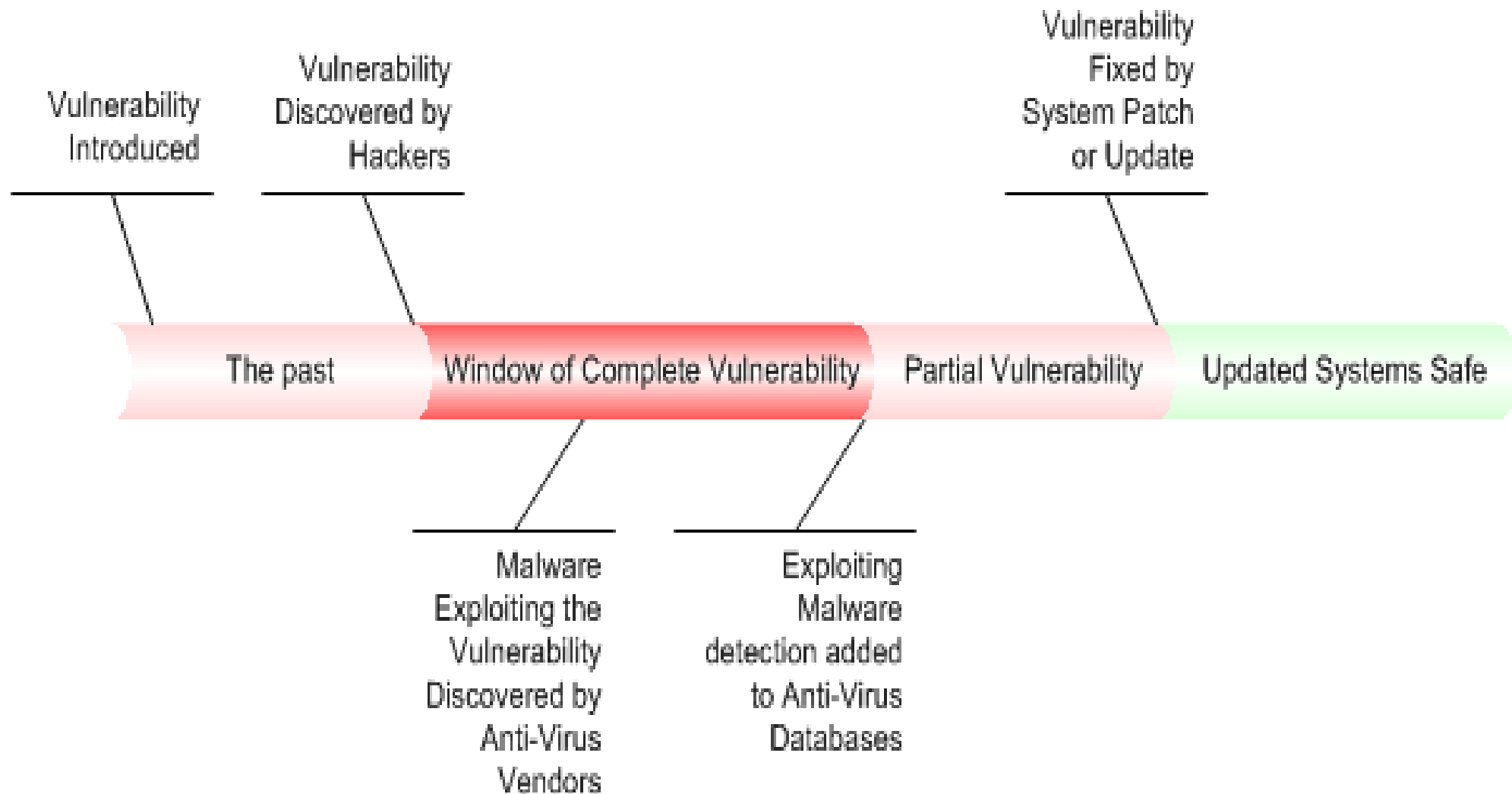
A partir de este momento, el tiempo que se tarde en dar una solución será el **tiempo de reacción**

De este tiempo de reacción depende la probabilidad de que la vulnerabilidad descubierta sea explotada para configurar un ataque



# Algo de terminología

- Ciclo de vida de las vulnerabilidades



## Algo de terminología

---

- **Riesgo:** posibilidad de que se materialice una amenaza aprovechando una vulnerabilidad
- **Ataque:** la materialización de una amenaza
- **Impacto:** consecuencia de de un ataque



# Informe de seguridad de Secunia (2011)

Las vulnerabilidades son resistentes

Ninguno de los Top20 productores de software ha conseguido reducir el número de vulnerabilidades en sus productos en 5 años

#	Vendor	History 2006-11	2011 CVEs	Risk	Trend 5yr	1yr
1	Novell		1,113		+81% ▲	+32% ▲
2	Red Hat		982		+45% ▲	-5% ▼
3	Canonical		625		+48% ▲	+9% ▲
4	Debian		563		+15% ▲	+33% ▲
5	Gentoo		523		+28% ▲	+154% ▲
6	Oracle		497		+27% ▲	+34% ▲
7	Apple		360		+12% ▲	-17% ▼
8	Google		324		+800% ▲	+116% ▲
9	Microsoft		231		+17% ▲	-20% ▼
10	VMware		205		+193% ▲	+63% ▲
11	IBM		192		+21% ▲	-19% ▼
12	Adobe		179		+106% ▲	-16% ▼
13	HP		175		+9% ▲	-34% ▼
14	Cisco		135		+41% ▲	+7% ▲
15	Mozilla		117		+26% ▲	+2% ▲
16	Kernel		81		+8% ▲	-21% ▼
17	Apache		45		+88% ▲	+18% ▲
18	Xerox		43		+330% ▲	+2050% ▲
19	Attachmate		41		+583% ▲	+273% ▲
20	Opera		41		+116% ▲	+28% ▲

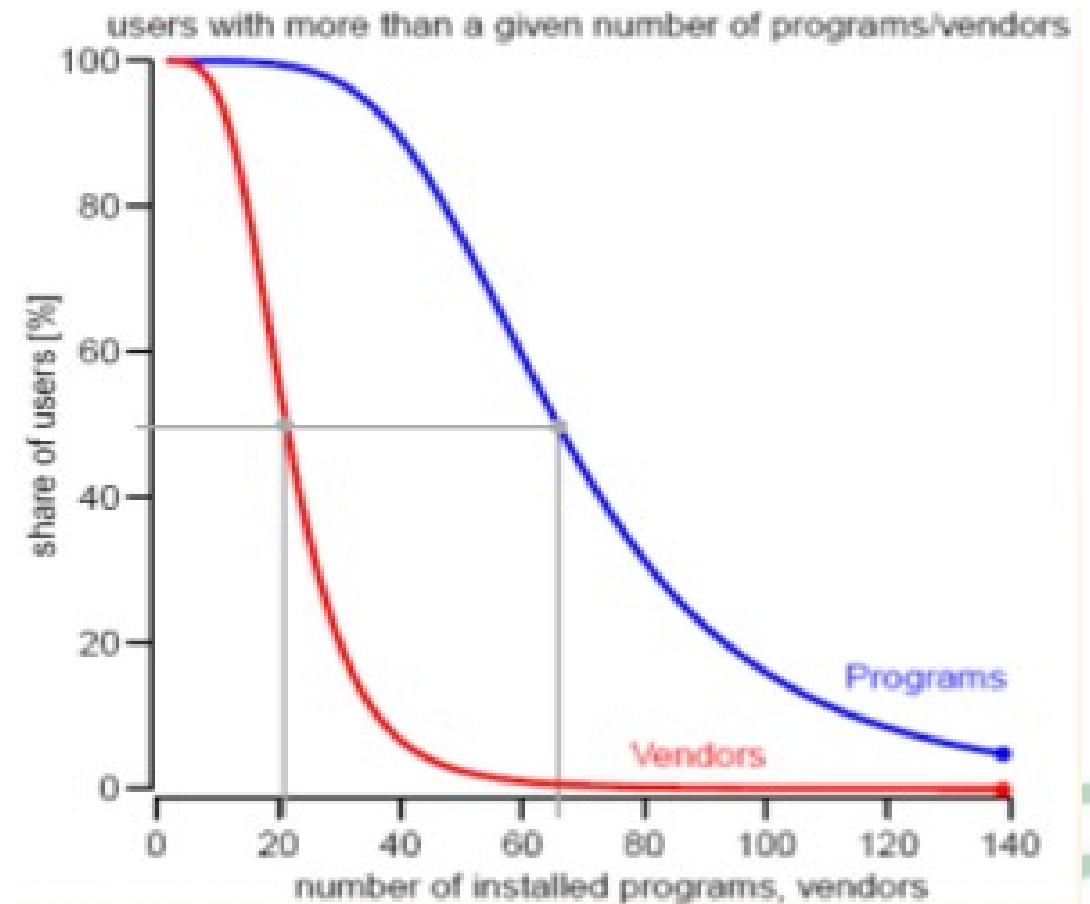
Fuente: Secunia Yearly Report 2011  
<http://secunia.com/resources/reports/>



# Informe de seguridad de Secunia (2011)

Las máquinas finales son objetivos lucrativos para los cibercriminales

Suelen estar poco protegidos, ya que son entornos dinámicos con un patrón de uso no predecible.



Fuente: Secunia Yearly Report 2011  
<http://secunia.com/resources/reports/>

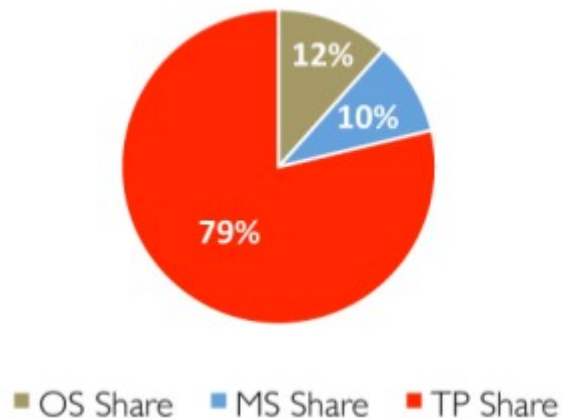
# Informe de seguridad de Secunia (2011)

---

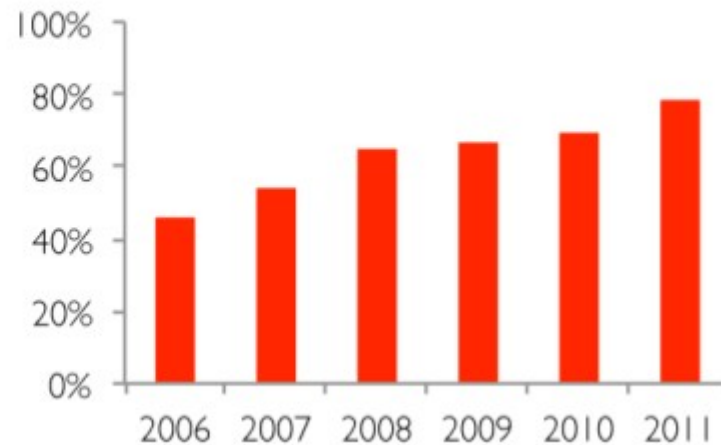
El software de Microsoft ya no es el objetivo principal

Los programas de terceros son los responsables casi en exclusiva del aumento de vulnerabilidades en equipos finales

Top-50 Portfolio  
Share of vulnerabilities by source



Share of vulnerabilities  
by third-party programs



**Fuente:** Secunia Yearly Report 2011  
<http://secunia.com/resources/reports/>

# Informe de seguridad de Secunia (2011)

---

La complejidad es el peor enemigo de la seguridad

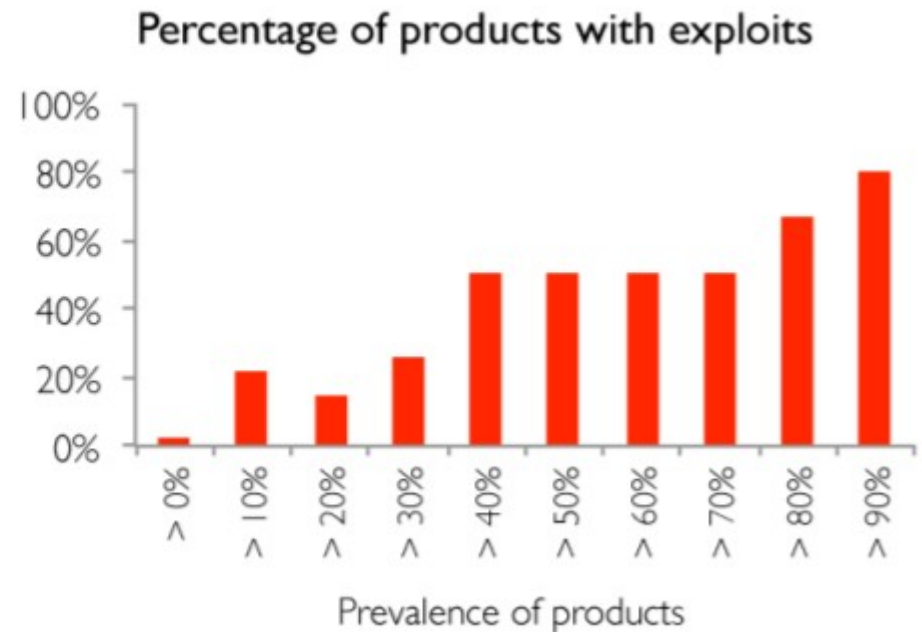
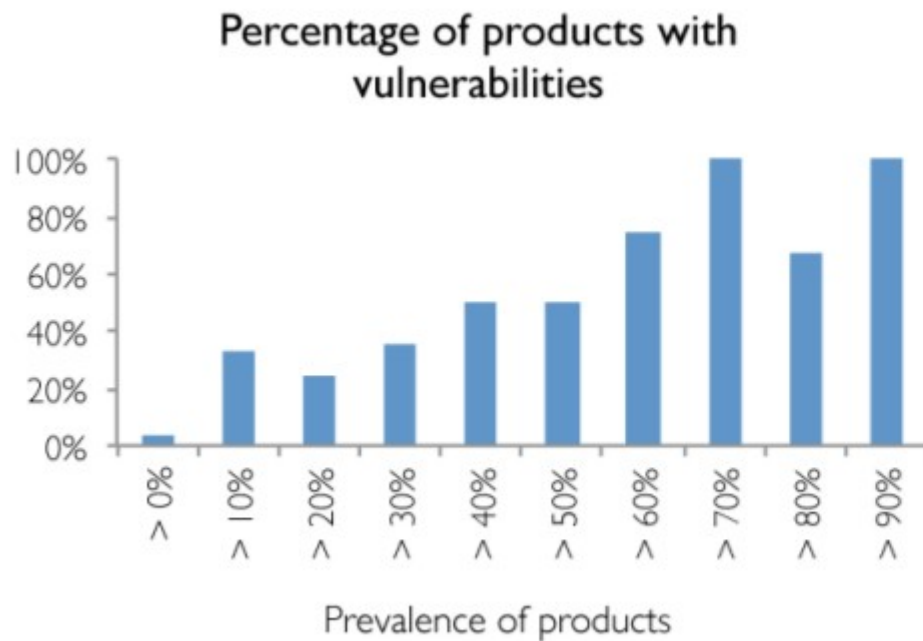
El Top-50 software portfolio instalado en un equipo final típico incluye programas de 12 fabricantes diferentes (28 programas Microsoft programs y 22 programas de terceros), lo que implica 12 mecanismos de actualización diferentes para mantener el equipo seguro (1 de Microsoft y 11 mecanismos adicionales)



**Fuente:** Secunia Yearly Report 2011  
<http://secunia.com/resources/reports/>

# Informe de seguridad de Secunia (2011)

No sólo los típicos programas presentan vulnerabilidades, las aplicaciones menos conocidas también pueden estar expuestas a los cibercriminales



**Fuente:** Secunia Yearly Report 2011  
<http://secunia.com/resources/reports/>

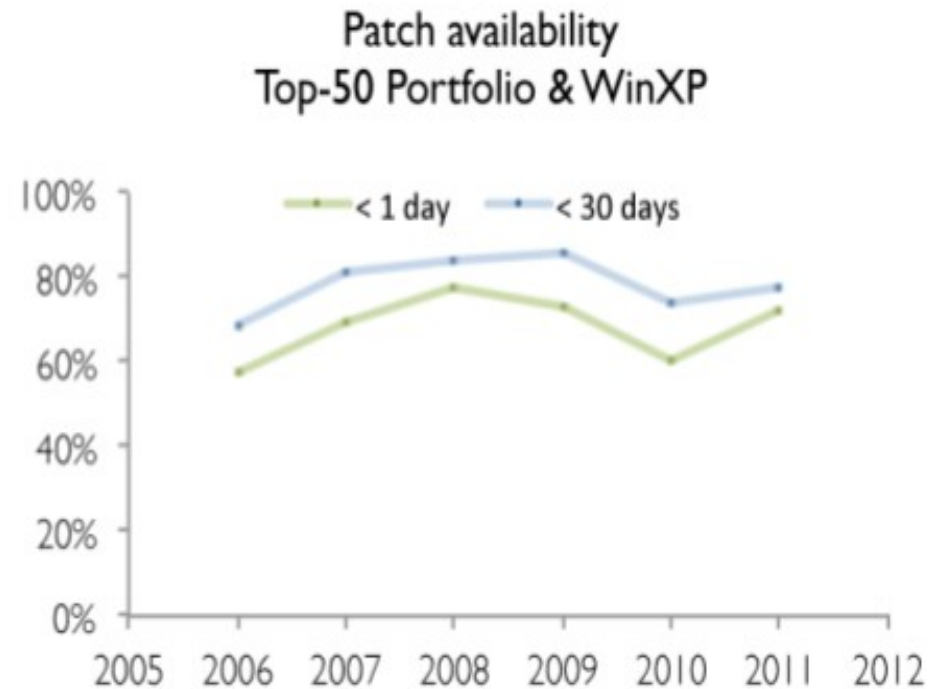
# Informe de seguridad de Secunia (2011)

---

Sin embargo, el

# 72%

de las vulnerabilidades tienen parches disponibles el día de su publicación, por lo que el poder de parchear y asegurar las máquinas finales queda en manos de los administradores.



**Fuente:** Secunia Yearly Report 2011  
<http://secunia.com/resources/reports/>

# Secunia PSI

---



Herramienta gratuita que detecta programas y plug-ins vulnerables y no actualizados que exponen el equipo a ataques

