

Sistema Intel·ligent de Gestió de Vulnerabilitats Informàtiques

Òscar Güell
Sebastián Gómez

gener de 2006

Resum

Eina desenvolupada per UPcnet utilitzant programari lliure, que permet detectar aplicacions afectades per alguna vulnerabilitat, notificar-les, i gestionar les alertes i les actualitzacions. L'objectiu principal és ajudar a l'administrador de sistemes en la detecció de les vulnerabilitats que puguin afectar a qualsevol dels seus sistemes, basant-se en un repositori del maquinari i programari instal·lat i en la gestió de la informació de les vulnerabilitats que cada dia és generada per diferents organitzacions.

1. Introducció

Dia rere dia, i des de fa ja molt de temps, augmenten les inversions i les infraestructures per part de les administracions i les empreses per millorar les comunicacions, optimitzar les existents i cercar noves tecnologies amb l'objectiu de migrar els models de negoci a d'altres més interessants pels resultats que generen basats en la informàtica i les comunicacions. El que es busca és, en definitiva, possibilitar i facilitar als usuaris finals l'accessibilitat als serveis que ofereixen les organitzacions bo i aprofitant les avantatges de les TIC.

A la nostra societat i en el nostre entorn, ric i pròsper, el nombre potencial d'usuaris que poden arribar a accedir als serveis que s'ofereixen són centenars de milions. Aquesta realitat, junt al fet que els models de negoci moderns depenen críticament de la disponibilitat dels seus serveis, condiona a que en el disseny de tots i cada un dels elements que intervenen entre l'usuari i el servei siguin objectius primordials la seguretat, la fiabilitat i la robustesa.

En qualsevol cas la seguretat total no existeix en absolut i malauradament cada any es publiquen milers d'avís alertant sobre errades de disseny en els elements TIC, errades que posen en perill les dades emmagatzemades, la disponibilitat dels serveis oferts i el que en definitiva preocupa més, la continuïtat dels processos de negoci de les empreses i/o organitzacions.

Sortosament però, en la gran majoria de casos aquestes alertes per vulnerabilitats arriben amb temps suficient per poder ser corregides abans que el risc es converteixi en una amenaça real o en un desastre. El problema esdevé quan toca processar l'avís i discernir si ens afecta o no. No seria un gran problema si la nostra organització utilitzés poques tecnologies, però malauradament la idiosincràsia del món de les TIC fan que grans i mitjanes organitzacions hagin d'utilitzar un ventall extremadament extens de tipus i models diferents de sistemes operatius, electrònica de xarxa, servidors d'aplicacions, bases de dades, etc.

Si als milers d'avís de vulnerabilitat anuals, els hi ajuntem el nombre d'aplicacions amb versions diferents (80.000 aproximadament) que existeixen actualment es desprèn que cal disposar d'un mecanisme ràpid i àgil

amb capacitat de resposta a aquestes situacions.

En la majoria dels casos el mecanisme “àgil” que es fa servir consisteix en un equip d'una o més persones especialitzades discriminant en el moment que arriba un avís de vulnerabilitat si els afecta o no i, en cas afirmatiu, quines accions han de prendre per solucionar-ho. En la resta de casos les organitzacions o bé no disposen de tècnics qualificats o simplement assumeixen el ris de no fer res.

Aquest cost humà, l'assumpció del riscs i les conseqüències de no fer una bona gestió de les vulnerabilitats es pot estalviar utilitzant el que hem batejat com Sistema Intel·ligent de Gestió de Vulnerabilitats Informàtiques (SIGVI).

2. Objectius de SIGVI

Per començar a explicar en que consisteix aquest projecte, un parell de definicions necessàries:

Vulnerabilitat: Qualsevol característica d'un sistema informàtic que possibilita que algú impedeixi el seu correcte funcionament o que permeti que un usuari no autoritzat es faci amb el control del sistema.

Administració de la vulnerabilitat: Pràctica consistent en identificar i eliminar els punts febles i susceptibles de comprometre la confidencialitat, integritat o disponibilitat d'un recurs informàtic. Pràctica de seguretat de la informació preventiva que identifica i elimina els punts febles abans de que siguin utilitzats per comprometre la seguretat d'un recurs informàtic.

2.1. Definició

El Sistema Intel·ligent de Gestió de Vulnerabilitats Informàtiques (SIGVI) és un aplicatiu de tipus client servidor altament configurable amb capacitat de gestionar i notificar en temps real els avisos per vulnerabilitat que realment afecten i interessen de qualsevol dels serveis i aplicacions d'una o varies organitzacions.

SIGVI s'alimenta automàticament de qualsevol servei internacional d'alertes de vulnerabilitat com els oferts per organitzacions com NVD [1] o CERT [2] i d'un inventari dels serveis de les organitzacions a gestionar per, en temps real i després de comprovar que es compleixen les condicions desitjades, avisar al client de l'existència d'una alerta en un dels seus serveis just quan aquesta apareix. A més, SIGVI permet als usuaris saber en qualsevol moment si les seves aplicacions pateixen alguna vulnerabilitat.

2.2. Antecedents

Al mercat mundial, a l'àmbit acadèmic o a l'àmbit del codi obert no existeix cap eina que tingui les mateixes característiques funcionals o que siguin remotament semblants a les de SIGVI, fent-la així única i veritablement innovadora.

Només durant els cinc darrers anys es van notificar 2.500 vulnerabilitats, i actualment hi ha 16.000 aplicacions amb versions diferents actives. Només en els dos primers mesos d'aquest any 2005, en nombre de casos nous avisos confirma l'augment que any rere any s'està produint. A la UPC la gran majoria d'incidències de seguretat sofertes es podrien haver evitat amb un sistema de control de vulnerabilitats com el que aquest projecte presenta.

2.3. Característiques innovadores de SIGVI

SIGVI és, per la seva pròpia definició, un projecte innovador ja que automatitza de forma senzilla un conjunt d'accions i processos que s'havien de realitzar manualment i que ningú abans ho havia posat en pràctica. A nivell de la UPC aquest projecte ofereix un nou, útil, innovador i necessari servei a tots els centres de càlcul i unitats estructurals de la comunitat.

A més, SIGVI ha estat especificat, dissenyat i el seu prototipus construït fent servir única i exclusivament eines amb llicència de codi obert, seguint l'esperit i la línia estratègica de la UPC.

Aquest projecte pot obrir una nova línia de negoci ja que es pot oferir a d'altres administracions externes bé oferint el producte o bé un servei.

SIGVI redueix enormement els riscos per oblits i errades humanes en general al automatitzar un procés on cal prendre decisions.

Estalvia recursos de la UPC i agilitza la consecució d'un estat de seguretat dels actius d'informació òptim. El sistema es distribuïble, facilitant així la segregació de responsabilitats en organitzacions complexes com la de la UPC o d'altres semblants.

SIGVI és multiusuari, permet que en una mateixa instància del projecte puguin beneficiar-se moltes organitzacions o, en el cas de la UPC, molts departaments, escoles o unitats estructurals. Totes elles poden gestionar les seves necessitats de manera independent a la resta de grups de la comunitat.

L'escalabilitat del projecte és enorme: amb molts pocs recursos pot oferir servei a molts usuaris i afegir-ne més no suposa augmentar els recursos de manera significativa.

La flexibilitat de SIGVI és total ja que cobreix les diferents necessitats de cada usuari oferint-los una eina de configuració pròpia del sistema per adaptar-lo a aquestes.

És intel·ligent per què es capaç d'aprendre de la informació que rep i prendre decisions posteriorment de forma automàtica.

És molt barat per què tot el programari emprat es lliure i per què per la part client només cal un navegador. Els requeriments de maquinari per la part servidora depenen del nombre d'usuaris, però el sistema no exigeix gaires recursos.

Fent una enumeració a mode de resum de les principals característiques del projecte tenim que:

- És innovador.
- És útil i necessari per la comunitat UPC.
- Millora la seguretat del actius d'informació.
- Estalvia recursos.
- Genera nou negoci.
- És 100% PL.
- Evita errors humans.
- És distribuïble.
- És multiusuari.
- És escalable.
- És flexible.
- És intel·ligent.
- És barat d'implantar.

3. Descripció de SIGVI

3.1. Mòduls principals

El disseny de SIGVI és completament modular i cada mòdul té definides una sèrie d'interfícies amb l'objectiu de flexibilitzar així totes les modificacions i totes les ampliacions que pugin ser necessàries per adaptar el producte a les necessitats finals del client.

S'utilitzen bàsicament tres bases de dades per gestionar totes les dades necessàries a cada uns dels fluxos de procés principals.

Els mòduls i les bases de dades que donen cos al sistema i que estan representades a la figura 1 amb les seves respectives interrelacions són:

- Mòdul de recepció de vulnerabilitats: és l'encarregat de rebre els avisos de vulnerabilitats i transmetre'ls al sistema per què els emmagatzemi i els processi. Cada avís genera un flux de processos. El mòdul permet utilitzar diferents interfícies de manera que pot ser programat per què actualitzi la informació periòdica i automàticament d'una font pública, actualitzar-la en arribar avisos e-mail, o per altres mètodes.
- Mòdul de gestió de serveis: és l'encarregat de transmetre al sistema quins serveis han de ser considerats quan es rebí un avís de vulnerabilitat. Aquest mòdul permet interfícies per fer consultes, altes, baixes i modificacions de forma manual pels administradors a través d'un formulari web. També, de forma automàtica, permet fer altes, baixes i modificacions amb un escaneig de xarxa.
- Mòdul de gestió d'alarmes: és l'encarregat de programar quins avisos i en quines circumstàncies han d'arribar als propietaris o administradors del servei.
- Mòdul de generació d'alarmes: és l'encarregat de generar l'alarma i enviar-la al propietari o administrador del servei.
- Base de dades de vulnerabilitats: conté totes les vulnerabilitats conegudes. La modifica el Mòdul de recepció de vulnerabilitats.
- Base de dades de serveis: conté tots els serveis que han de ser comprovats. La modifica el Mòdul de gestió de serveis.
- Base de dades d'alarmes: conté totes les alarmes generades i el seu estat, així com en quines circumstàncies s'han de generar les alertes. És modificada pel Mòdul de gestió d'alarmes.
- SIGVI kernel: és el cervell del sistema i l'encarregat de gestionar les relacions entre els mòduls i les bases de dades. Es pot programar per dotar-lo de capacitat IA.

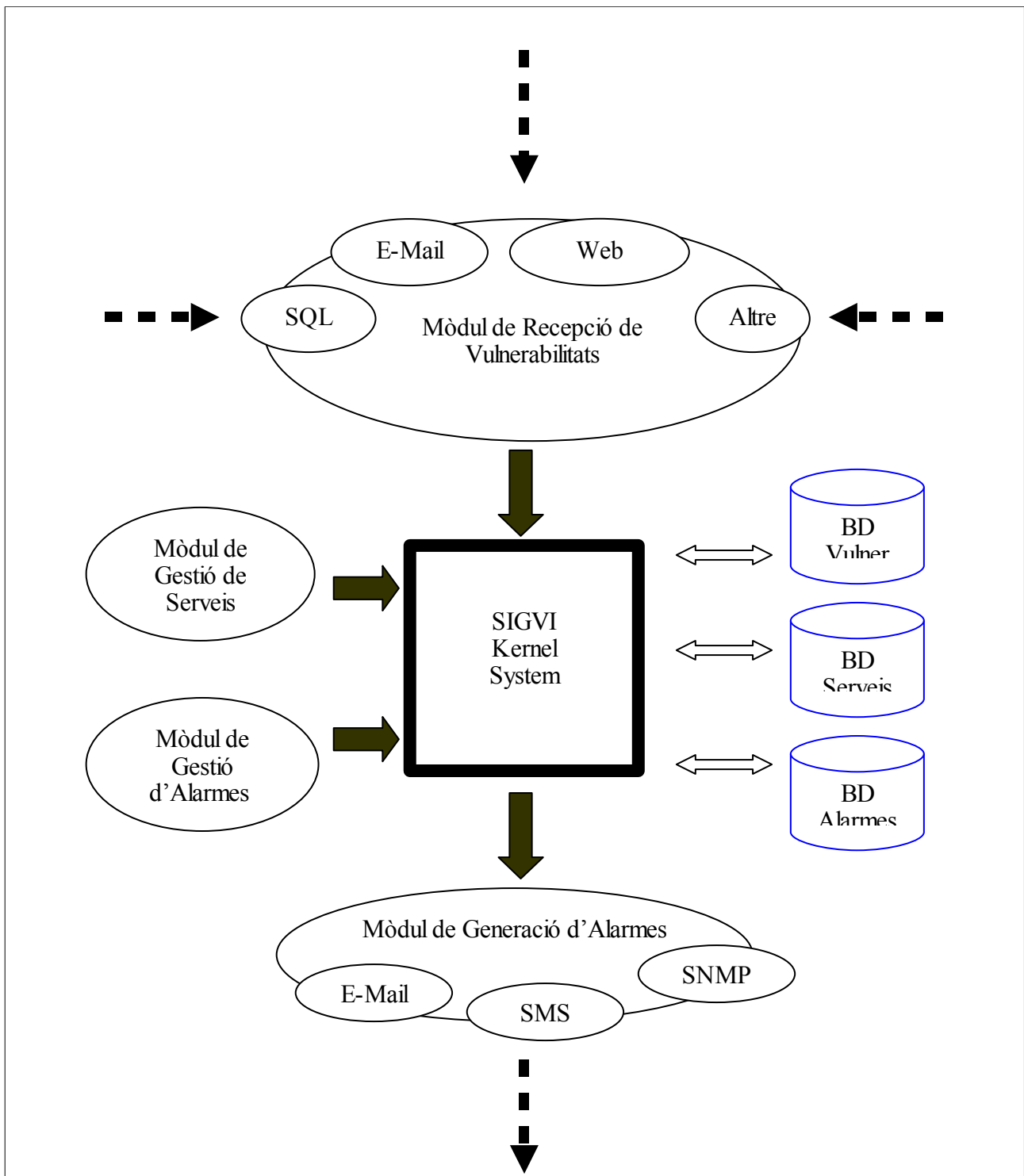


Figura 1. Visió modular de SIGVI.

A part d'aquests mòduls i bases de dades, són necessaris altres complementaris per poder realitzar estadístiques, gestionar usuaris, perfils i grups, etc.

3.2. Funcionalitats

A mode resum, un usuari donat d'alta a SIGVI pot realitzar entre d'altres tasques:

- Consultar l'estat de vulnerabilitat de qualsevol dels serveis propis que tingui donats d'alta al sistema.
- Canviar l'estat de vulnerabilitat del seus serveis.
- Donar d'alta, baixa o modificar qualsevol del seus serveis.
- Consultar i modificar les condicions que s'han de donar per rebre un avís del sistema: tipus de vulnerabilitat, grau de perillositat, etc.
- Seleccionar la persona o persones que cal notificar en cas necessari i la via que els sistema ha de prendre per fer-ho.
- Consultar els històrics dels seus serveis.
- Generar estadístiques.

Els usuaris amb perfil d'administradors poden per la seva banda fer altes d'usuaris finals, així com donar d'alta manualment vulnerabilitats en cas que sigui necessari.

A més el sistema donarà facilitats a l'usuari final a l'hora de donar d'alta els seus serveis oferint un analitzador remot de serveis.

La intel·ligència del sistema ve donada per la capacitat que se li pot donar per a aprendre de cara a situacions posteriors de les decisions preses per l'usuari quan accepta o rebutja una alerta.

3.3. Model de processos

Per no presentar tots els possibles casos, i com a mostra del model de processos del sistema a continuació es descriu un parell d'escenaris bàsics:

- Alta d'una nova vulnerabilitat:

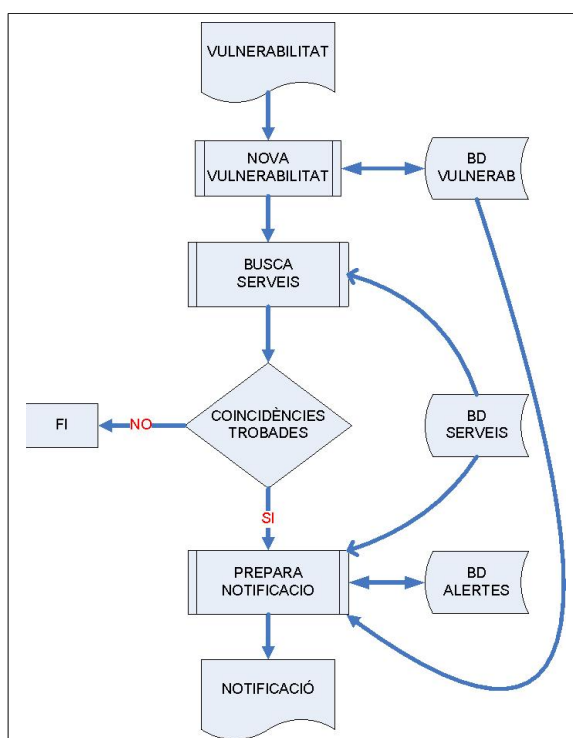


Figura 2. Flux de processos d'un alta de vulnerabilitat

- Alta d'un nou servei:

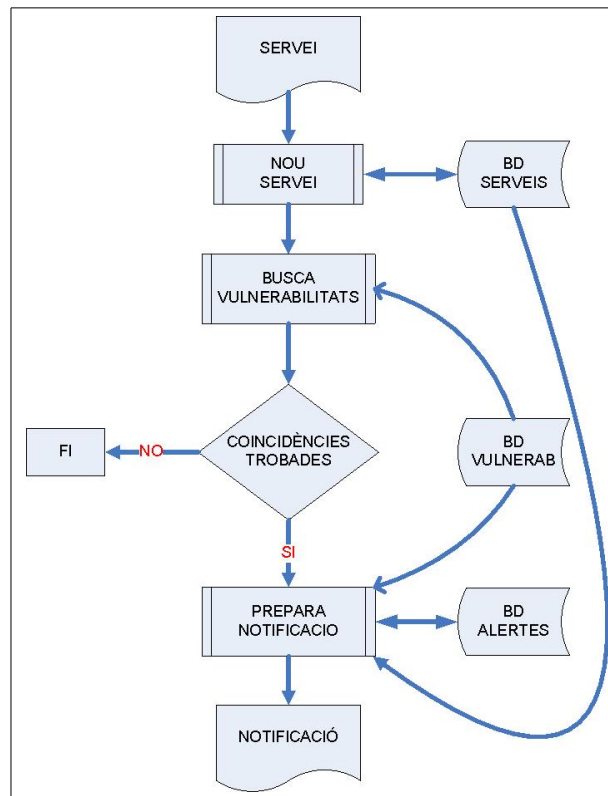


Figura 3. Flux de processos d'un alta de Servei.

4. Estat actual de desenvolupament


Aquest projecte va resultar guanyador de la primera edició del Premi Davyd Luque a la Innovació en les TIC, al març de 2005, i per demostrar la seva viabilitat es va desenvolupar un pilot. Darrerament s'ha dut a terme el desenvolupament i actualment es troba en semi-explotació a UPCnet.

Les eines de desenvolupament i de funcionament emprades han estat:


1. Debian Linux
2. Servidor web Apache v.2
3. SGBD MySQL
4. PHP

Tota la informació sobre el projecte així com la descàrrega de la primera versió està publicada a La Farga de la UPC [3] i a SourceForge [4].

Algunes pantalles capturades són:



Gestió de vulnerabilitats


UNIVERSITAT POLITÈCNICA
DE CATALUNYA

Gestio de Vulnerabilitats


Menu principal	
• Estat de les vulnerabilitats dels servidors	

Administracio	
• Index	
• Manteniment dels usuaris	
• Manteniment dels grups	
• Manteniment dels servidors	
• Manteniment dels productes als servidors	


Eines	
Vulnerabilitats	
• Carregar la llista de vulnerabilitats a la BBDD	
• Manteniment de les Vulnerabilitats	
Productes	
• Carregar la llista de productes a la BBDD	
• Manteniment dels productes	
Comprovacio de l'estat	
• Revisar les vulnerabilitats dels servidors	

Home

Figura 4. Pantalla inicial SIGVI



Gestió de vulnerabilitats


UNIVERSITAT POLITÈCNICA
DE CATALUNYA

Gestió de vulnerabilitats::Tools::vulnerabilitats

Servidor	Empresa	Producte	Id. vulnerabilitat	Risc	Descripcio
cerberush	Red Hat Linux	Red Hat Linux, 9	CAN-2003-0364	Medium	The TCP/IP fragment reassembly handling in the Linux kernel 2.4 allows remote attackers to cause a denial of service (CPU consumption) via certain packets that cause a large number of hash table collisions
cerberush	OpenSSH	OpenSSH, 3.7.1p1	CAN-2003-0787	High	The PAM conversation function in OpenSSH 3.7.1 and 3.7.1p1 interprets an array of structures as an array of pointers, which allows attackers to modify the stack and possibly gain privileges.
cerberush	OpenSSH	OpenSSH, 3.7.1p1	CAN-2003-0786	High	The SSH1 PAM challenge response authentication in OpenSSH 3.7.1 and 3.7.1p1, when Privilege Separation is disabled, does not check the result of the authentication attempt, which can allow remote attackers to gain privileges.
ts.upc.es	Microsoft	Windows 2000 Server, SP3	CAN-2004-0726	High	The Windows Media Player control in Microsoft Windows 2000 allows remote attackers to execute arbitrary script in the local computer zone via an ASX filename that contains javascript, which is executed in the local context in a preview panel.
merovingio	SuSE	Linux Enterprise Server, 9	CAN-2004-0883	Medium	Multiple vulnerabilities in the samba filesystem (smbfs) in Linux kernel 2.4 and 2.6 allow remote samba servers to cause a denial of service (crash) or gain sensitive information from kernel memory via a samba server (1) returning more data than requested to the smb_proc_read function, (2) returning a data offset from outside the samba packet to the smb_proc_readX function, (3) sending a certain TRANS2 fragmented packet to the smb_receive_trans2 function, (4) sending a samba packet with a certain header size to the smb_proc_readX_data function, or (5) sending a certain packet based offset for the data in a packet to the smb_receive_trans2 function.
merovingio	SuSE	Linux Enterprise Server, 9	CAN-2004-0886	Medium	Multiple integer overflows in libtiff 3.6.1 and earlier allow remote attackers to cause a denial of service (crash or memory corruption) via TIFF images that lead to incorrect malloc calls.
ts.upc.es	Microsoft	Windows 2000 Server, SP3	CAN-2004-0893	High	The Local Procedure Call (LPC) interface of the Windows Kernel for Windows NT 4.0, Windows 2000, Windows XP, and Windows Server 2003 does not properly validate the lengths of messages sent to the LPC port, which allows local users to gain privileges, aka Windows Kernel Vulnerability.
ts.upc.es	Microsoft	Windows 2000 Server, SP3	CAN-2004-0894	High	LSASS (Local Security Authority Subsystem Service) of Windows 2000 Server and Windows Server 2003 does not properly validate connection information, which allows local users to gain privileges via a specially-designed program.
merovingio	SuSE	Linux Enterprise Server, 9	CAN-2004-0902	High	Multiple heap-based buffer overflows in Mozilla Firefox before the Preview Release, Mozilla before 1.7.3, and Thunderbird before 0.8 allow remote attackers to cause a denial of service (application crash) or execute arbitrary code via (1) the Send page functionality, (2) certain responses from a malicious POP3 server, or (3) a link containing a non-ASCII hostname.
merovingio	SuSE	Linux Enterprise Server, 9	CAN-2004-0903	High	Stack-based buffer overflow in the writeGroup function in nsVCardObj.cpp for Mozilla Firefox before the Preview Release, Mozilla before 1.7.3, and Thunderbird before 0.8 allows remote attackers to execute arbitrary code via malformed VCard attachments that are not properly handled when previewing a message.

Figura 5. Base de dades d'alertes.

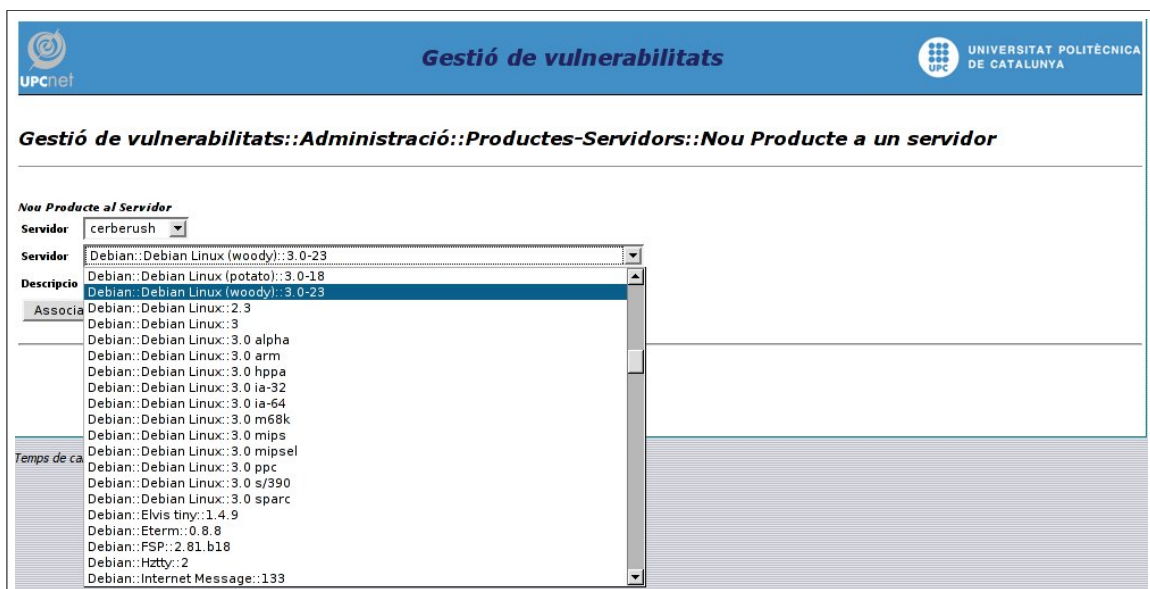


Figura 6. Mòdul de Gestió de Serveis

5. Costos del projecte

Tots els costos que es presenten són reals, i els de la part d'exploració estan calculats per donar servei a la comunitat UPC.

Cost de desenvolupar el projecte:

Maquinari: 0 €
 Programari: 0 €
 RRHH: 50 hores TGS
 230 hores TGM

Cost d'implantar el servei:

Maquinari: 3.000 €
 Programari: 0 €
 RRHH: 20 hores TGM

Cost de manteniment:

RRHH: 60 hores/any TGM

6. Conclusions

Veiem que el SIGVI és una eina molt útil i a la llarga pràcticament imprescindible. Alhora creiem que el plantejament de desenvolupar-la en programari lliure i seguint un mètode de desenvolupament en comunitat, li donarà valor i la podrà fer servir molta més gent.

Referències

- [1] NVD, National Vulnerability Database, National Institute of Standards and Technology -- <http://nvd.nist.gov/>
- [2] CERT – Computer Emergency Response Team, Carnegie Mellon University -- <http://www.cert.org/>
- [3] La Farga de la UPC -- <https://lafarga.cpl.upc.edu/projects/sigvi/>
- [4] Sourceforge -- <http://sigvi.sourceforge.net/>