Debian Security Team

16 dicembre 2005

Dipartimento di Informatica e Scienze dell'Informazione

Emanuele Rocca - ema@debian.org
http://people.debian.org/~ema/talks/

Debian Security Team

- Introduzione al progetto Debian
- Problematiche di sicurezza
- Security Team
- Advisory (DSA)
- Collaborazione con altri vendor
- Un po' di numeri
- Testing Security Team
- Security Audit Project

il progetto Debian

The Debian Project is an association of individuals who have made common cause to create a free operating system.

pacchetti Debian

file binari contenenti software libero (DFSG)
opportunamente adattato a Debian
(FHS, Debian Policy...)

la versione originale del software viene detta
“upstream”, così come l'autore (upstream author)

Esempio: *mysql*
4.1.15 upstream
4.1.15-1 debian

Rilasci

UNSTABLE (sid)
dove avviene lo sviluppo quotidiano

TESTING (etch)
pacchetti non ancora rilasciati come stabili

STABLE (sarge)
l'ultima versione Debian rilasciata
solo *stable* viene seguita dal Security Team

il progetto Debian

- 11 architetture
- 1635 sviluppatori
- 16763 pacchetti
- più di 50.000.000 di linee di codice

problematiche di sicurezza

Una vulnerabilità di sicurezza in uno dei circa 16000 pacchetti Debian costituisce una problematica di sicurezza per l'intera distribuzione.

Se ne prende carico il Debian Security Team, una volta appurato che la vulnerabilità sia davvero presente nella release stabile.

il Debian Security Team

Compiti:

- monitoraggio mailing list di sicurezza
  - bugtraq
  - vuln-dev
- verifica dell'applicabilità delle vulnerabilità alla release stabile
- punto di contatto tra:
  - sviluppatori upstream
  - organismi di sicurezza (CERT, CVE...)
  - altre distibuzioni
- rilascio Debian Security Advisory

Debian Security Advisories

Quando viene scoperta una vulnerabilità che si applica ad un pacchetto Debian, il team di sicurezza rilascia un advisory contentente informazioni sulla vulnerabilità

I DSA sono inviati alle mailing-list debian-security-announce@lists.debian.org e bugtraq

A partire dal 2004 i DSA sono stati dichiarati compatibili CVE (Common Vulnerability Exposures)

Common Vulnerabilities and Exposures

Certificate of CVE® Compatibility

for

Software in the Public Interest, Inc.'s
Debian Security Advisories

In accordance with the Requirements and Recommendations for CVE Compatibility, version 1.0.0, the CVE Program hereby awards the label of CVE-Compatible as of 24 February 2004.

Robert A. Martin
Compatibility Lead

M. Margaret Zuk
Program Manager

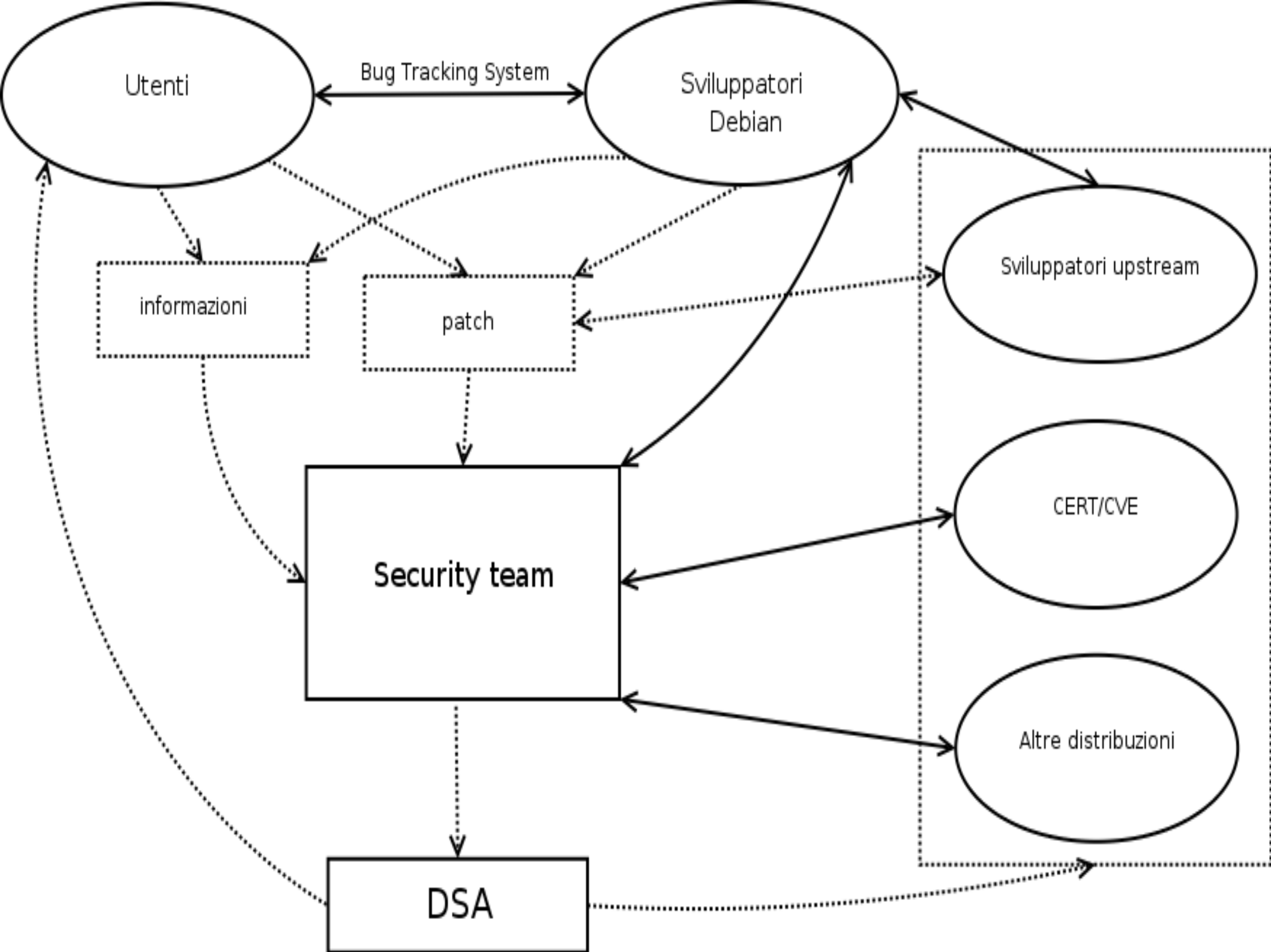
Steven M. Christey
Technical Lead

Compatibilità CVE

CVE è un dizionario di nomi standardizzati per le vulnerabilità

Associare una generica vulnerabilità ad aggiornamenti Debian specifici

Semplificare la gestione della sicurezza negli ambienti in cui si usano strumenti CVE-enabled (IDS, strumenti di vulnerability assessment)

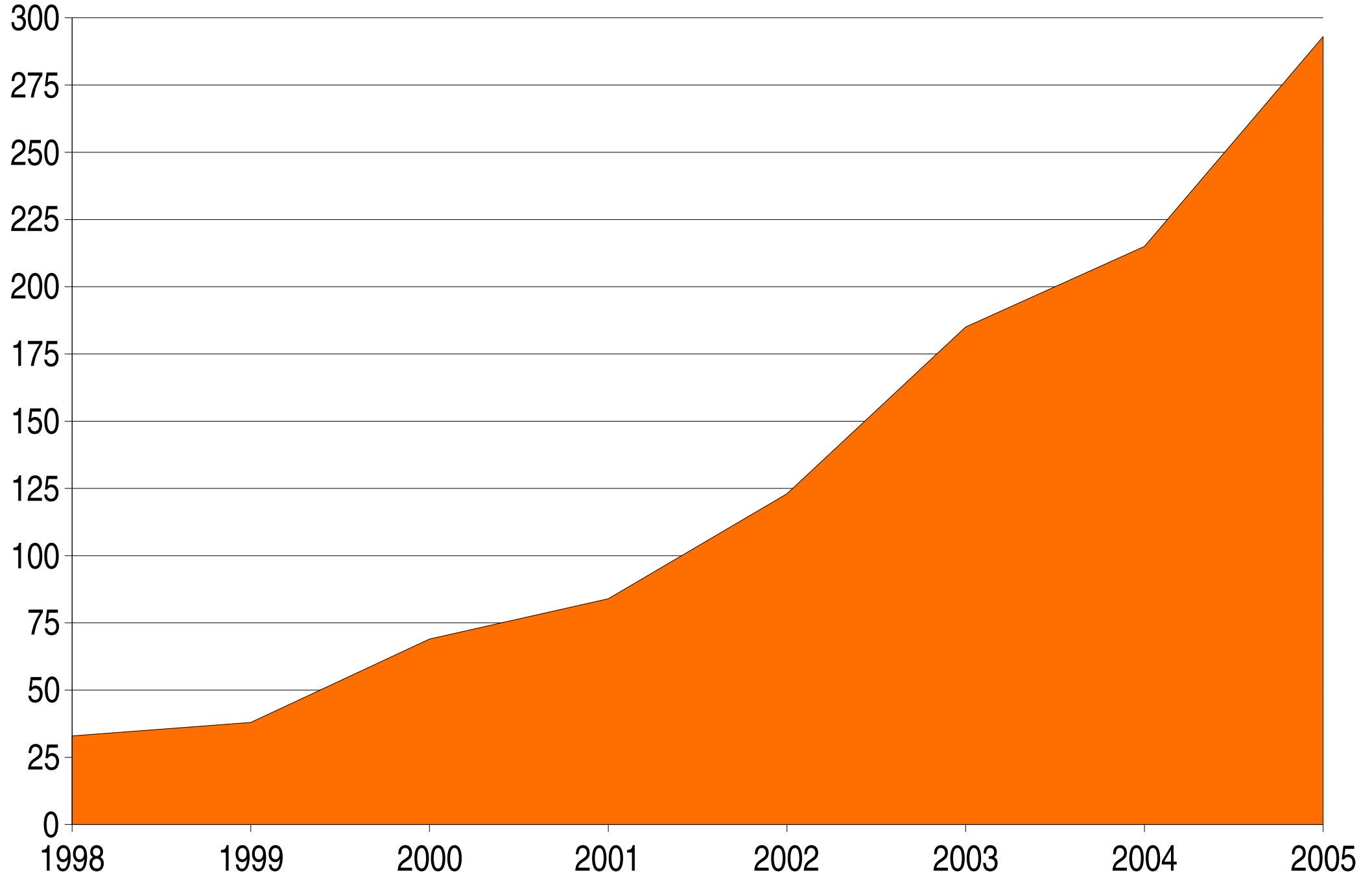

Utenti
Bug Tracking System
Sviluppatori Debian
Sviluppatori upstream
informazioni
patch
Security team
CERT/CVE
Altre distribuzioni
DSA

Debian Security Advisories

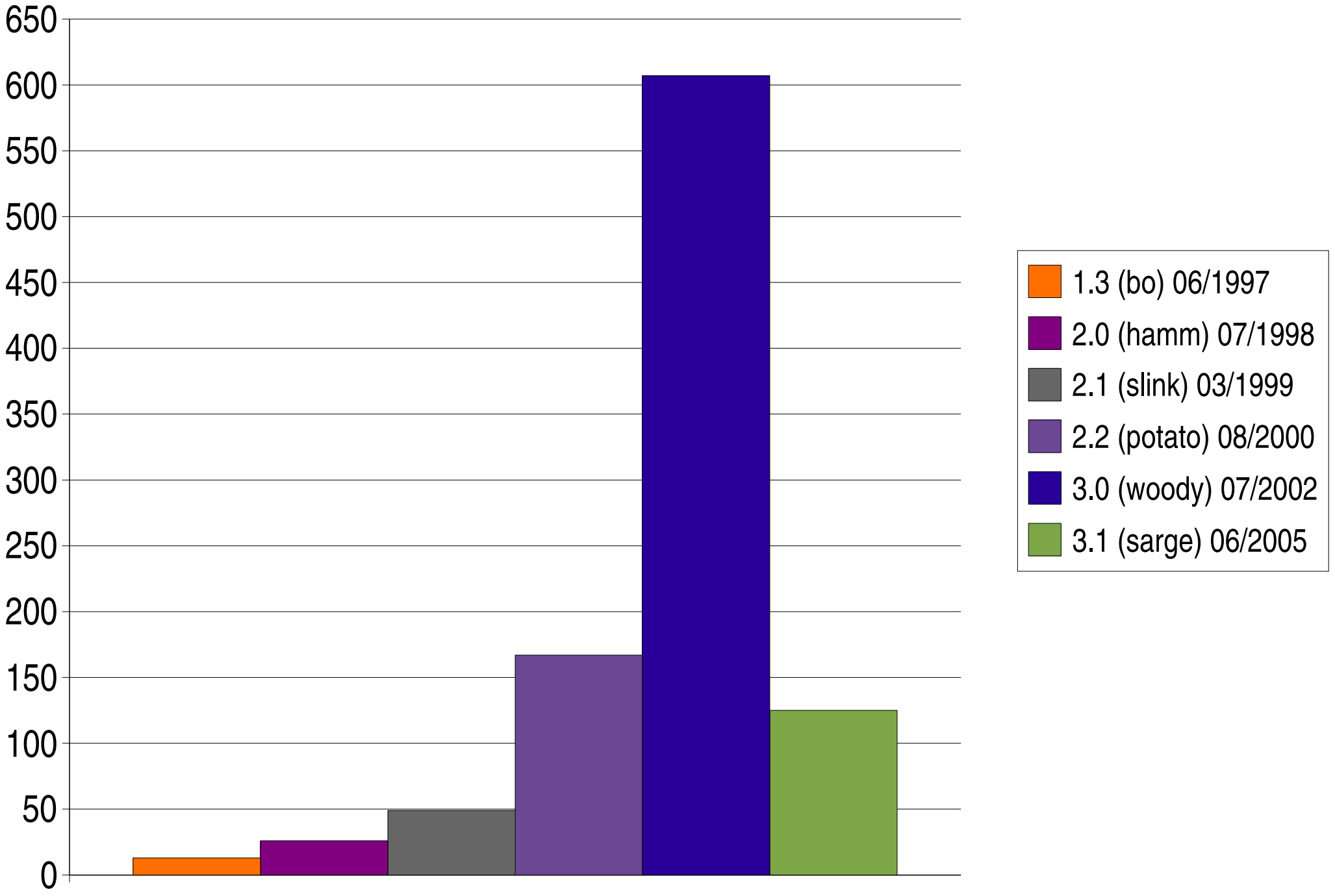
- numero di versione del pacchetto aggiornato
- tipo di problema
- remoto / locale
- descrizione del pacchetto
- descrizione del problema
- descrizione dell'exploit
- descrizione del fix
- md5sum e indirzzo dei pacchetti aggiornati

Andiamo a vedere un esempio

Andamento annuale DSA



Andamento DSA per release



Flusso eventi

- Il Security Team viene a conoscenza di un problema di sicurezza che si applica ad un pacchetto presente in Debian Stable
- Viene contattato lo sviluppatore Debian
- Fix del problema, meno “invasivo” possibile
- Caso migliore: qualcuno ha già preparato una nuova versione Debian del pacchetto che chiude il problema
- Caso peggiore: il Security Team deve scrivere la patch
- Testing (exploit, test di regressione...)
- Upload del pacchetto su security.debian.org
- Advisory

Riservatezza?

Di solito no.

Possono esserci, comunque, casi specifici che richiedano omertà assoluta da parte del Security Team

- Vulnerabilità non ancora pubblica
- Vulnerabilità grave

In questo caso il Security Team lavora insieme alle altre distribuzioni (RedHat, Suse...) al fine di produrre fix, advisory e aggiornamenti

Testing Security Team

Come abbiamo visto, non c'è supporto di sicurezza per Debian Testing.

Sempre più utenti “desktop” usano Debian Testing, è un peccato lasciarli senza aggiornamenti.

Il Debian Testing Security Team nasce appunto per supplire a questa mancanza.

Audit project

- Il progetto si occupa di fare auditing dei pacchetti Debian, alla ricerca di problemi di sicurezza
- 45 DSA rilasciati ad oggi grazie al lavoro dei membri dell'Audit project
- Approccio proattivo
- Priorità:
  - binari setuid/setgid
  - servizi di rete
  - cgi/php
  - cron script eseguiti con privilegi alti

Riferimenti

- http://security.debian.org/
- http://www.debian.org/security/faq
- http://www.debian.org/security/crossreferences
- http://cve.mitre.org/about/
- http://cve.mitre.org/cve/refs/refmap/source-DEBIAN.html
- http://www.kb.cert.org/vuls/
- http://www.securityfocus.com/bid
- http://secure-testing-master.debian.net/
- http://www.debian.org/security/audit/