3ème année

Sécurité des Systèmes Informatiques

SUPAERO

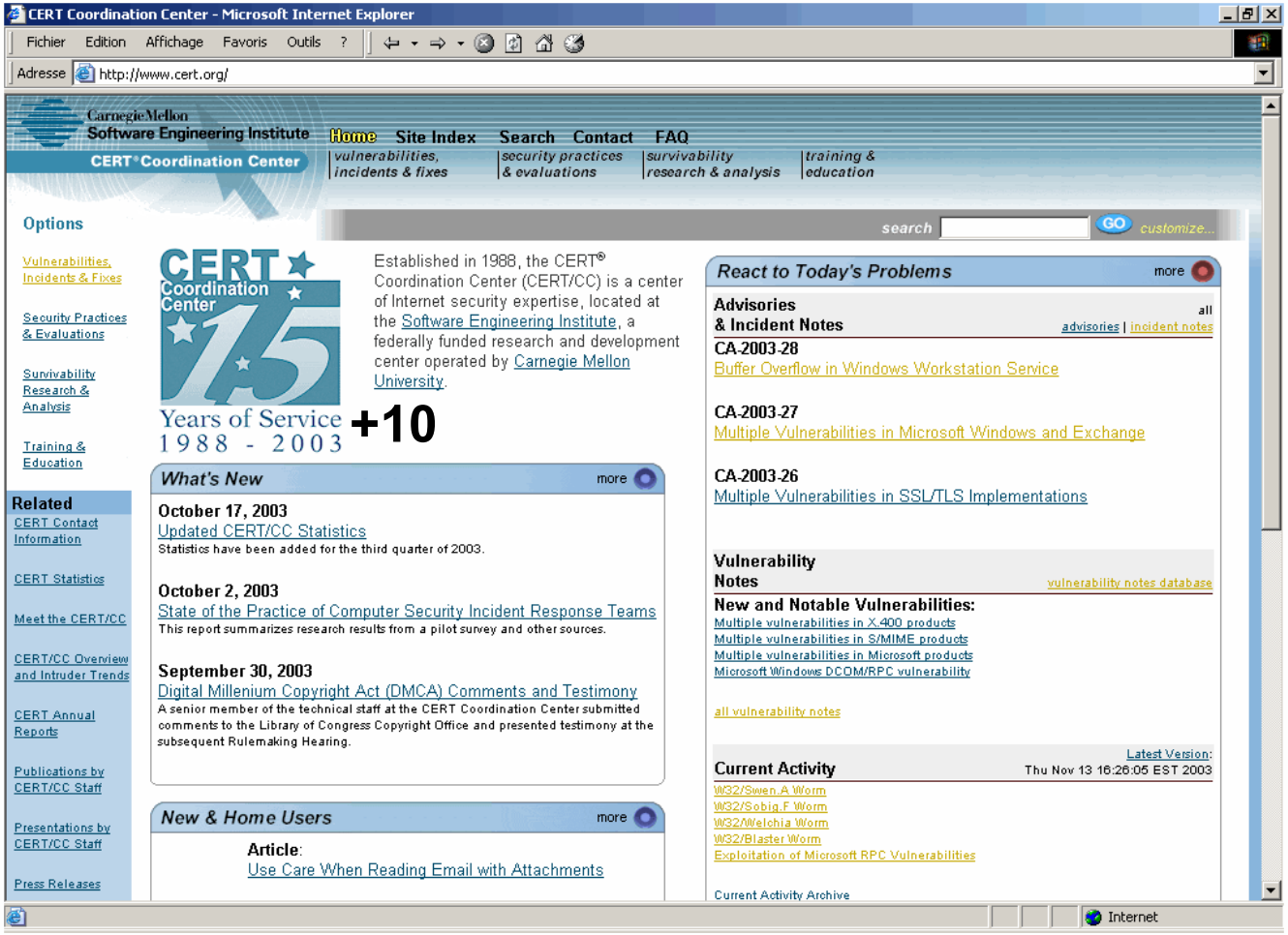
Rodolphe Ortalo
CARSAT Midi-Pyrénées
rodolphe.ortalo@free.fr
(rodolphe.ortalo@carsat-mp.fr)
http://rodolphe.ortalo.free.fr/ssi.html

Plan (1/2)

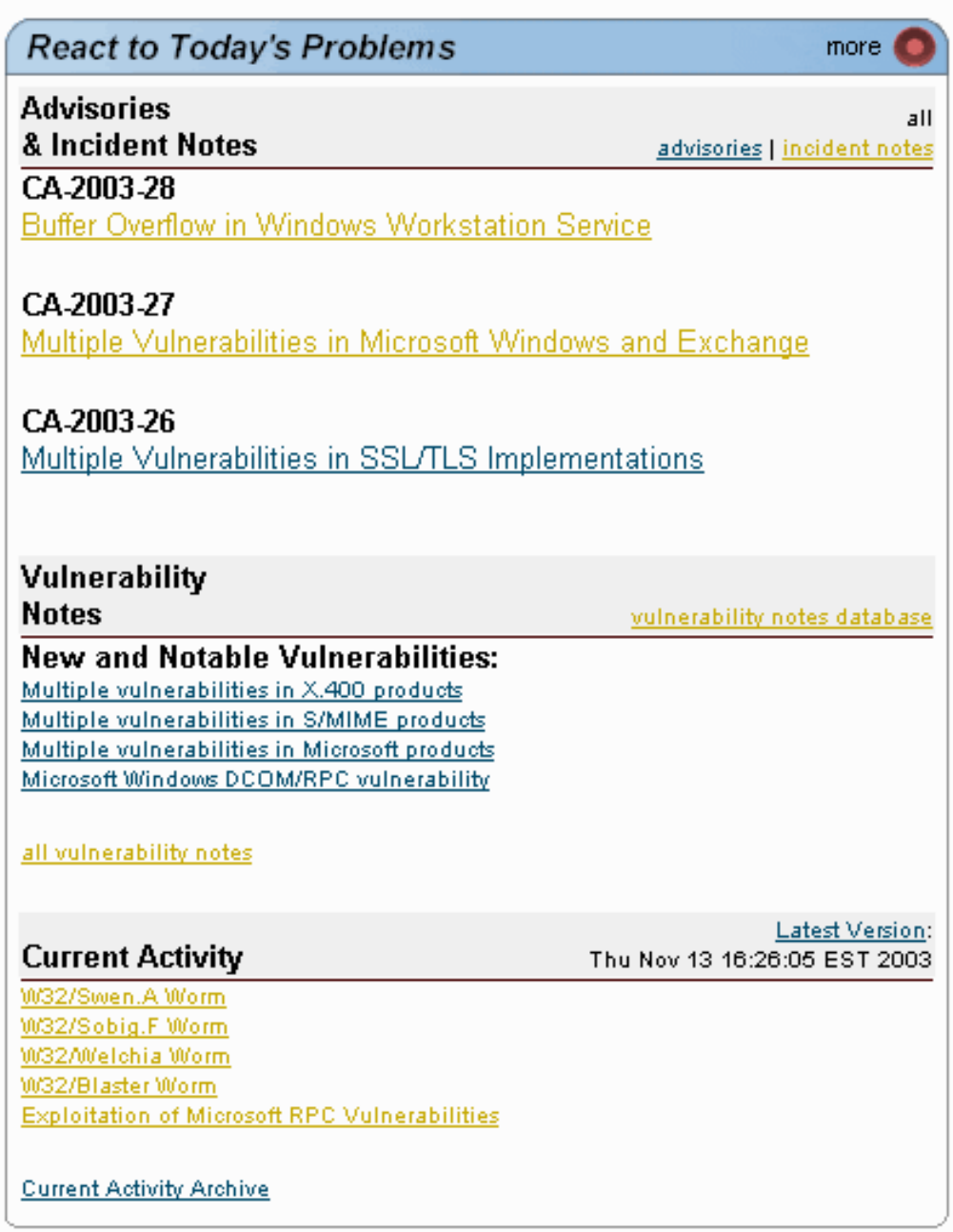
- Généralités
  - Propriétés de sécurité
  - Attaques
- Mise en œuvre dans les organisations
  - Fonctionnement de la sécurité dans une entreprise
  - **Suivi des alertes de sécurité**
  - Définition d'un schéma directeur sécurité
- Mécanismes de protection généraux
  - Cryptographie
  - Politiques de sécurité formelles
  - Critères d'évaluation normalisés

Le CERT
Computer Emergency Response Team

www.cert.org



Principales informations diffusées



React to Today's Problems more

Advisories & Incident Notes
all
advisories | incident notes

CA-2003-28
Buffer Overflow in Windows Workstation Service

CA-2003-27
Multiple Vulnerabilities in Microsoft Windows and Exchange

CA-2003-26
Multiple Vulnerabilities in SSL/TLS Implementations

Vulnerability Notes
vulnerability notes database

New and Notable Vulnerabilities:
Multiple vulnerabilities in X.400 products
Multiple vulnerabilities in S/MIME products
Multiple vulnerabilities in Microsoft products
Microsoft Windows DCOM/RPC vulnerability

all vulnerability notes

Current Activity
Latest Version:
Thu Nov 13 16:26:05 EST 2003

W32/Swen.A Worm
W32/Sobig.F Worm
W32/Welchia Worm
W32/Blaster Worm
Exploitation of Microsoft RPC Vulnerabilities

Current Activity Archive

Les avis et notes du CERT

- Avis (exemples)
  - CERT Advisory CA-2003-28 (Microsoft)
  - CERT Advisory CA-2003-26 (SSL/TLS)
- Base de vulnérabilités
  - CERT VU#567620 (de CA-2003-28 et Microsoft MS03-049) http://www.kb.cert.org/vuls/id/567620
  - CA-2003-26 est associé à 6 vulnérabilités
  - CERT VU#936868 (Oracle et réplique) http://www.kb.cert.org/vuls/id/936868
  - Avis constructeurs et autres: http://www.debian.org/security/2004/dsa-419

Tous les avis

Fiche CERT : Principaux éléments

- *Title / Overview*
- *Systems affected*
- *Description*
- *Impact*
- *Solution*
- *References*
- *Credit / Vendor Info. / Other Info.*

La série Blaster (été 2003)

- CERT VU#568148
- CERT Advisory CA-2003-16
- Microsoft MS03-026
- CERT Advisory CA-2003-19
- CERT Advisory CA-2003-20
- CERT Current Activity (Blaster)

L'actualité plus récente

- CERTA, l'année 2011 (au hasard) :
  - Page principale

  - La dernière blague de Windows
  - Back to SSL conception
  - etc.

- Remarque/Question
  - Pourrais-je réutiliser le transparent l'année prochaine?
    (Ex. A, Ex. B, Ex. C)

CVE

Le vrai changement?

CVE-ID Syntax Change

Old Syntax

CVE-YYYY-NNNN

4 fixed digits, supports a maximum of 9,999 unique identifiers per year.

Fixed 4-Digit Examples

CVE-1999-0067
CVE-2005-4873
CVE-2012-0158

New Syntax

CVE-YYYY-NNNN...N

4-digit minimum and no maximum, provides for additional capacity each year when needed.

Arbitrary Digits Examples

CVE-2014-0001
CVE-2014-12345
CVE-2014-7654321

YYYY indicates year the ID is issued to a CVE Numbering Authority (CNA) or published.

Implementation date: January 1, 2014

Source: http://cve.mitre.org