

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

The screenshot shows the CERT Coordination Center website in a Microsoft Internet Explorer browser window. The address bar displays <http://www.cert.org/>. The page header includes the Carnegie Mellon Software Engineering Institute logo and navigation links: Home, Site Index, Search, Contact, and FAQ. A search bar is located in the top right corner.

The main content area features a large graphic celebrating 15 years of service (1988-2003) with a '+10' overlay. Below this, the 'What's New' section lists recent updates:

- October 17, 2003**: [Updated CERT/CC Statistics](#). Statistics have been added for the third quarter of 2003.
- October 2, 2003**: [State of the Practice of Computer Security Incident Response Teams](#). This report summarizes research results from a pilot survey and other sources.
- September 30, 2003**: [Digital Millennium Copyright Act \(DMCA\) Comments and Testimony](#). A senior member of the technical staff at the CERT Coordination Center submitted comments to the Library of Congress Copyright Office and presented testimony at the subsequent Rulemaking Hearing.


The 'New & Home Users' section includes an article: [Use Care When Reading Email with Attachments](#).

The 'React to Today's Problems' section lists advisories and 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](#)

Additional sections include 'Vulnerability Notes' with links to [Multiple vulnerabilities in X.400 products](#), [Multiple vulnerabilities in S/MIME products](#), [Multiple vulnerabilities in Microsoft products](#), and [Microsoft Windows DCOM/RPC vulnerability](#). The 'Current Activity' section is dated Thu Nov 13 16:28:05 EST 2003 and lists items like [W32/Swen.A Worm](#), [W32/Sobig.F Worm](#), [W32/Welchia Worm](#), [W32/Blaster Worm](#), and [Exploitation of Microsoft RPC Vulnerabilities](#).

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>