Cooperación Inteco - NIST

Peter Mell

National Vulnerability Database Project Lead

Senior Computer Scientist

NIST Computer Security Division

Tim Grance

Manager, Systems and Network Security Group

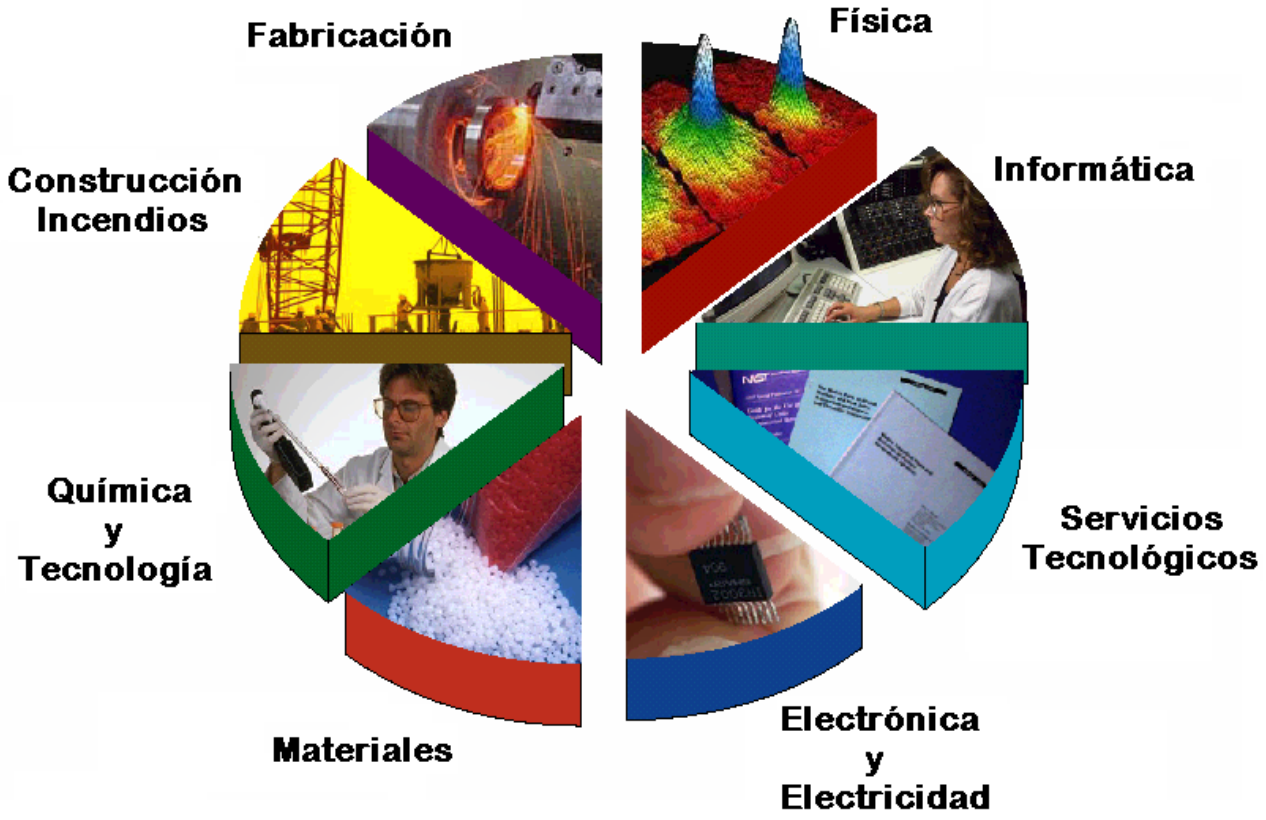
NIST Computer Security Division

20 de julio de 2006

NIST (National Institute of Standards and Technology)

El objetivo de NIST es desarrollar y promover medidas, normas y tecnología para aumentar la productividad, facilitar el comercio y mejorar la calidad de vida.

- **3,000 empleados**
- **1,600 investigadores asociados**



NIST División de Seguridad Informática

- **Criptografía / Autenticación**
  - Estándares y aplicaciones criptográficas.
  - Herramientas criptográficas estándar.
  - Autenticación electrónica.
- **Chequeo de Seguridad**
  - Módulo criptográfico del programa de validación.
  - Guía de validación 800-53A
- **Gestión de la Seguridad**
  - Estándares federales e industriales de seguridad.
  - Guías de gestión de la Seguridad.
  - Revisiones del programa de la Agencia.
- **Tecnologías de Seguridad**
  - Listas de chequeo de la Seguridad.
  - Guías técnicas de Seguridad.
  - Programa gubernamental de Tarjetas inteligentes (*Smart Card*).
  - Seguridad en dispositivos móviles.
  - Análisis forense.
  - Control de acceso y gestión de la autorización.
  - Base de Datos Nacional de Vulnerabilidades.
  - Protocolos y Servicios
  - Detección de Intrusiones.
  - Tecnología inalámbrica.

Descripción de la BBDD Nacional de Vulnerabilidades

La NVD (*National Vulnerability Database*) es una detallada Base de Datos de vulnerabilidades de tecnologías de la información que integra todos los recursos públicamente disponibles del gobierno de los EE.UU. sobre vulnerabilidades y los relaciona con recursos de la industria.

- 18200 resúmenes de vulnerabilidades.
- 2.2 millones de accesos cada mes.
- 17 vulnerabilidades nuevas cada día.

National Vulnerability Database

a comprehensive cyber vulnerability resource

Welcome to NVD!!

NVD is a comprehensive cyber security vulnerability database that integrates all publicly available U.S. Government vulnerability resources and provides references to industry resources. It is based on and synchronized with the CVE vulnerability naming standard.

Resource Status

NVD contains:
18263 CVE Vulnerabilities
61 US-CERT Alerts
1384 US-CERT Vuln Notes
1162 Oval Queries
Last updated:
07/14/06
Publication rate:
17 vulnerabilities / day

Search CVE Vulnerability Database

(Perform Advanced Search)

Keyword search: Search All

Try a product or vendor name
Try a CVE standard vulnerability name or OVAL query
Only vulnerabilities that match ALL keywords will be returned
Linux kernel vulnerabilities are categorized separately from vulnerabilities in specific Linux distributions

Search last 3 months | Search last 3 years

Show only vulnerabilities that have the following associated resources:

- ☐ US-CERT Technical Alerts
- ☐ US-CERT Vulnerability Notes
- ☐ OVAL Queries

Recent CVE Vulnerabilities

CVE-2006-3590 **Publish Date:** 7/14/2006
Unspecified vulnerability in mso.dll, as used by Microsoft PowerPoint 2000 through 2003, allows remote user-complicit attackers to execute arbitrary commands via a crafted PPT file, which causes a "memory corruption error," and exploited by Trojan.PPDropper.B. NOTE: As of 20060714, due to the vagueness of the initial disclosure, it is uncertain whether this is related to CVE-2006-1540 or CVE-2006-3493.

CVE-2006-1309 **Publish Date:** 7/13/2006
Microsoft Excel 2000 through 2004 allows user-complicit attackers to execute arbitrary code via a .xls file with a crafted LABEL record that triggers memory corruption.

CVE-2006-1308 **Publish Date:** 7/13/2006

National Cyber-Alert System

Vulnerability Summary CVE-2005-1208

Original release date: 6/14/2005
Last revised: 10/20/2005
Source: US-CERT/NIST

Overview

Integer overflow in Microsoft Windows 98, 2000, XP SP2 and earlier, and Server 2003 SP1 and earlier allows remote attackers to execute arbitrary code via a crafted compiled Help (.CHM) file with a large size field that triggers a heap-based buffer overflow, as demonstrated using a "ms-its:" URL in Internet Explorer.

Impact

CVSS Severity: 10 (High) Approximated
Range: Remotely exploitable
Impact Type: Provides administrator access

References to Advisories, Solutions, and Tools

US-CERT Technical Alert: TA05-165A
Name: TA05-165A
Type: Advisory , **Patch Information**
Hyperlink: http://www.us-cert.gov/cas/techalerts/TA05-165A.html

US-CERT Vulnerability Note: VU#851869
Name: VU#851869
Type: Advisory , **Patch Information**
Hyperlink: http://www.kb.cert.org/vuls/id/851869

Vulnerable software and versions

Microsoft, Windows 2000
Microsoft, Windows 98
Microsoft, Windows XP, Tablet PC Edition SP2
Microsoft, Windows XP, Tablet PC Edition SP1
Microsoft, Windows XP, Tablet PC Edition
Microsoft, Windows XP, SP2
Microsoft, Windows XP, SP1
Microsoft, Windows XP, Professional SP2
Microsoft, Windows XP, Professional SP1
Microsoft, Windows XP, Professional 64-bit
Microsoft, Windows XP, Professional
Microsoft, Windows XP, Media Center Edition SP2
Microsoft, Windows XP, Media Center Edition SP1
Microsoft, Windows XP, Media Center Edition
Microsoft, Windows XP, Home SP2
Microsoft, Windows XP, Home SP1
Microsoft, Windows XP, Home
Microsoft,
Microsoft,
Microsoft,
Microsoft,
Microsoft,
Microsoft,
Microsoft,
Microsoft,

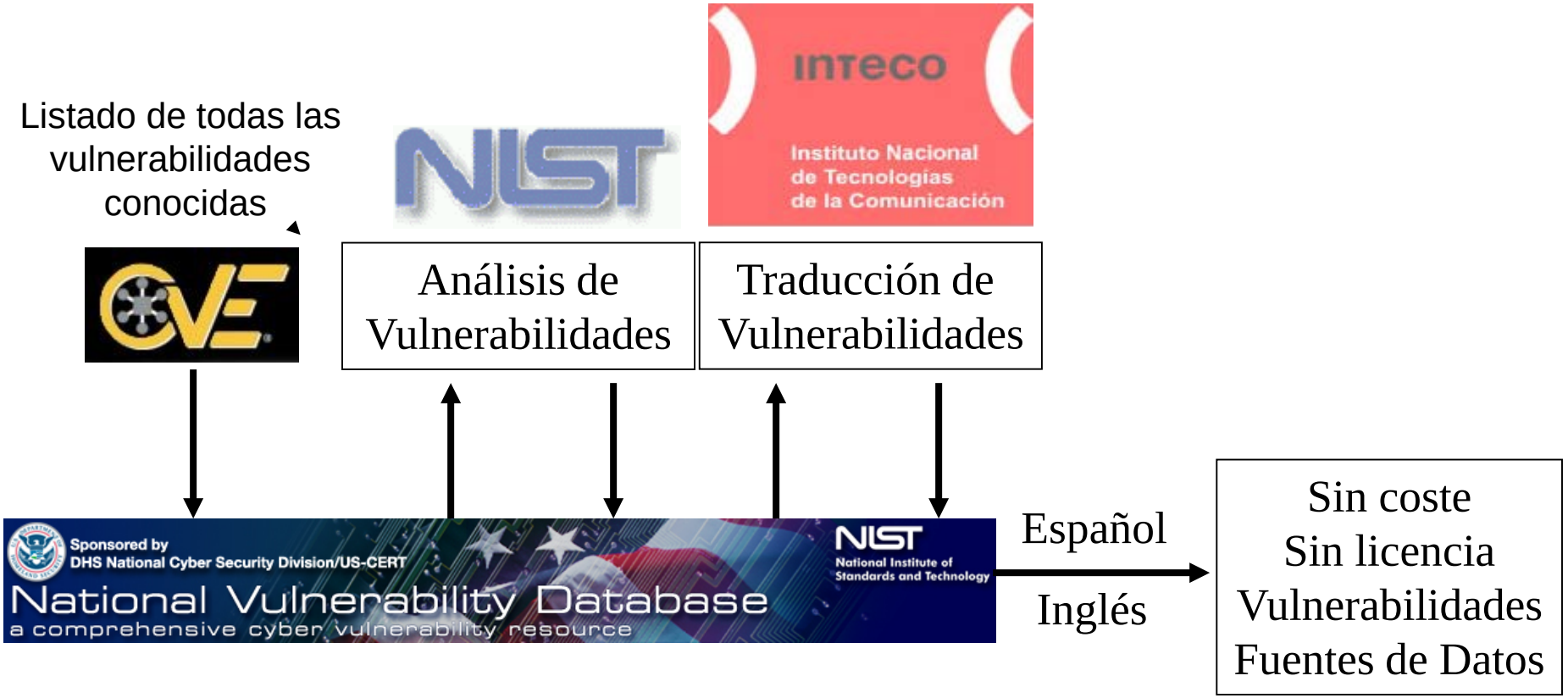
Technical Details

CVSS Base Score Descriptor: (AV:R/AC:L/Au:NR/C:C/I:C/A:C/B:N) Approximated

Vulnerability Type: Buffer Overflow

CVE Standard Vulnerability Entry:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-1208

Capacidades de exportación de NVD

- Fuentes RSS
  - Permite a los administradores de sistemas y al personal de operaciones de seguridad mantenerse actualizado sobre las últimas vulnerabilidades.
- Fuentes XML
  - Permite importar la información de las vulnerabilidades de la NVD desde otros productos.
  - La base de datos completa.
  - Sin restricciones de licencia.

Modo de Operación