

# National Vulnerability Database (NVD)

*Information Security and Privacy  
Advisory Board  
November 3-5, 2010*

Chris Johnson  
Computer Security Division  
Information Technology Laboratory  
The National Institute of Standards and  
Technology (NIST)



# Agenda

---

- National Vulnerability Database (NVD) Overview
- NVD Components
- NVD Analysis Activities
- NVD Data Feeds
- National Checklist Program (NCP)
- Security Content Automation Protocol (SCAP)  
Resources

# NVD Overview

---

- U.S. government repository of IT vulnerability information
- NVD database currently contains >44,000 vulnerability entries
- Website received over 40 million hits in CY 2009
- NVD data holdings are used extensively by government, industry and academia

# NVD Components

---

- National Vulnerability Database
  - Security-related software flaws
  - IT product dictionary
- National Checklist Program Website
  - Repository of low level checklists for securing operating systems and applications
- SCAP Validation Program Website
  - List of products that conform to the NIST-published SCAP validation requirements
- SCAP Resources
  - SCAP publications, data repositories and tools

# NVD Vulnerability Analysis Activities

---

- NVD contains over 44,000 Common Vulnerabilities and Exposures (CVE®) entries with the NVD Analysis Team analyzing ~6,000 vulnerabilities a year
  - ☞ Compute and publish impact metrics (i.e., Common Vulnerability Scoring System [CVSS] base scores)
  - ☞ Express affected platforms (e.g., software & versions) using a uniform naming convention – the Common Platform Enumeration
  - ☞ Describe the underlying weakness or root cause (e.g., buffer overflow, input validation error) of the software flaw using the Common Weakness Enumeration
  - ☞ Mediate vendor comments and community feedback

# NVD Advanced Search Capabilities

National Vulnerability Database (NVD) Advanced Search Vulnerabilities

http://web.nvd.nist.gov/view/vuln/search-advanced?cid=2

National Vulnerability Database  
automating vulnerability management, security measurement, and compliance checking

Vulnerabilities | Checklists | 800-53 Controls | Product Dictionary | Impact Metrics | Data Feeds | Statistics

Home | SCAP | SCAP Validated Tools | SCAP Events | About | Contact | Vendor Comments

### Mission and Overview

CVE and CCE Vulnerability Database Advanced Search

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

### Resource Status

NVD contains:

- 44254 [CVE Vulnerabilities](#)
- 162 [Checklists](#)
- 207 [US-CERT Alerts](#)
- 2422 [US-CERT Vuln Notes](#)
- 6057 [OVAL Queries](#)
- 26755 [CPE Names](#)

**Last updated:** Tue Nov 02 13:46:05 EDT 2010  
**CVE Publication rate:** 15.1

### Email List

NVD provides four mailing lists to the public. For information and subscription instructions please visit [NVD Mailing Lists](#)

### Workload Index

Vulnerability [Workload Index](#): 7.22

### About Us

NVD is a product of the [NIST Computer Security Division](#) and is sponsored by the Department of Homeland Security's [National Cyber Security Division](#). It supports the U.S. government multi-agency (OSD, DHS, NSA, DISA, and NIST) Information Security...

**Vulnerability Criteria**

**Software Flaws (CVE)**  
 **Misconfigurations (CCE), under development**

**CVE Identifier:**

**Keyword (text search):**

**Category (CWE):**

**CPE Name**

**Vendor:** [A..B](#) [C..E](#) [F..H](#) [I..K](#) [L..N](#) [O..Q](#) [R..T](#) [U..W](#) [X..Z](#) [All](#)

**Product:** [A..B](#) [C..E](#) [F..H](#) [I..K](#) [L..N](#) [O..Q](#) [R..T](#) [U..W](#) [X..Z](#) [All](#)

**Published Date Range**

**Start Date:**

**End Date:**

**Last Modified Date Range**

**Start Date:**

**End Date:**

**CVSS Version 2 Metrics**

**Severity (Base Score Range):**

**Access Vector:**

**Access Complexity:**

**Authentication:**

**Confidentiality:**

**Integrity:**

**Availability:**

**Hyperlinks**

- [US-CERT Technical Alerts](#)
- [US-CERT Vulnerability Notes](#)
- [OVAL Queries](#)

# NVD Vulnerability Summary

National Vulnerability Database (NVD) National Vulnerability Database (CVE-2010-4095)

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-4095

Most Visited: NIST VPN Inside NIST NIST Computer Security NIST Messaging NVD ITL Emergency/Safety NIST Virtual Library AMD - COTR DoC CLC NIST CLC Web Stats JIRA SCAP Issue Tra... Time & Attendance Travel Manager 9.0 ... NetLibrary - Basic S...

National Vulnerability Database (NVD) National Cyber-Alert System

**Mission and Overview**

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

**Vulnerability Summary for CVE-2010-4095**

**Original release date:** 10/26/2010  
**Last revised:** 10/28/2010  
**Source:** US-CERT/NIST

**Overview**

Directory traversal vulnerability in the FTP client in Serengeti Systems Incorporated Robo-FTP 3.7.3, and probably other versions before 3.7.5, allows remote FTP servers to write arbitrary files via a ... (dot dot) in a filename in a server response.

**Resource Status**

**NVD contains:**

- 44254 CVE Vulnerabilities
- 162 Checklists
- 207 US-CERT Alerts
- 2422 US-CERT Vulnerability Notes
- 6057 Publications
- 26755 CVE Names

**Last updated:** Tue Nov 02 14:01:06 EDT 2010  
**CVE Publication rate:** 15:1

**Email List**

NVD provides four mailing lists to the public. For information and subscription instructions please visit [NVD Mailing Lists](#).

**Workload Index**

Vulnerability Workload Index: 7.42

**About Us**

NVD is a product of the NIST Computer Security Division and is sponsored by the Department of Homeland Security's National Cyber Security Division. It supports the U.S. government multi-agency (OSD, DHS, NSA, DISA, and NIST) Information Security Automation Program. It is the U.S. government content repository for the Security Content Automation Protocol (SCAP).

**External Source:** XF

**Name:** roboftp-ftp-dir-traversal(62548)  
**Hyperlink:** <http://xforce.iss.net/xforce/xfdb/62548>

**External Source:** BID

**Name:** 44073  
**Hyperlink:** <http://www.securityfocus.com/bid/44073>

**External Source:** BUGTRAQ

**Name:** 20101013 Directory Traversal Vulnerability in Robo-FTP  
**Hyperlink:** <http://www.securityfocus.com/archive/1/archive/1/514267/100/0/threaded>

**External Source:** MISC

**Name:** [http://www.htbridge.ch/advisory/directory\\_traversal\\_vulnerability\\_in\\_robo\\_ftp.html](http://www.htbridge.ch/advisory/directory_traversal_vulnerability_in_robo_ftp.html)  
**Hyperlink:** [http://www.htbridge.ch/advisory/directory\\_traversal\\_vulnerability\\_in\\_robo\\_ftp.html](http://www.htbridge.ch/advisory/directory_traversal_vulnerability_in_robo_ftp.html)

**External Source:** SECUNIA

**Name:** 41809  
**Type:** Advisory  
**Hyperlink:** <http://secunia.com/advisories/41809>

**External Source:** CONFIRM

**Name:** [http://kb.robo-ftp.com/change\\_log/show/77](http://kb.robo-ftp.com/change_log/show/77)  
**Hyperlink:** [http://kb.robo-ftp.com/change\\_log/show/77](http://kb.robo-ftp.com/change_log/show/77)

**Vulnerable software and versions**

**Configuration 1**

- OR
- cpe:/a:robo-ftp:robo-ftp:3.7.3
- cpe:/a:robo-ftp:robo-ftp:3.7.4

\* Denotes Vulnerable Software  
 \* Changes related to vulnerability configurations

**Technical Details**

**Vulnerability Type** [\[View All\]](#)  
 Path Traversal (CWE-22)

**CVE Standard Vulnerability Entry:** <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4095>

REPORT A VULNERABILITY  
 REPORT AN INCIDENT

NIST  
 Computer Security  
 Division  
 1155  
 http://www.nist.gov

CVE  
 cve.mitre.org

CCE  
 Common Configuration Enumeration

CPE  
 Common Platform Enumeration

CVSS  
 CCDF

Done

# NVD Data Feeds

---

- Machine-readable vulnerability data feeds
  - >23,000 downloads of the NVD vulnerability data feeds in July 2010
- Product dictionary containing over 26,000 unique product names
  - 992 downloads of the NVD CPE dictionary file in July 2010
- Spanish language vulnerability data feeds (translations performed by INTECO personnel)
- Beta Common Configuration Enumeration (CCE) to 800-53 mappings

# National Checklist Program (NCP)

---

- NCP website contains 162 low-level checklists that are categorized as follows:
  - Tier I – Prose checklists
  - Tier II – Non-SCAP automated content
  - Tier III – Designed to work in an SCAP-validated tool
  - Tier IV – Will work in an SCAP-validated tool
- Checklist submissions come from a variety of organizations – government agencies, software vendors and third parties
- Submission guidelines for the NCP are described in NIST Special Publication 800-70, Rev. 1; National Checklist Program for IT Products-Guidelines for Checklist Users and Developers

# SCAP Resources

---

- SCAP Publications
  - ☞ NIST SP 800-117: Guide to Adopting and Using the Security Content Automation Protocol
  - ☞ NIST SP 800-126: The Technical Specification for the Security Content Automation Protocol
  - ☞ NIST IR 7511: Security Content Automation Protocol (SCAP) Validation Program Test Requirements
- SCAP Content Development Tools
  - ☞ Enhanced SCAP Editor (eSCAPE)
  - ☞ Recommendation Tracker
  - ☞ SCAP Content Validation Tool

# SCAP Validation Program Website

---

- List of products that have been validated by NIST as conforming to the SCAP and its component specifications
- Full description of SCAP product validation information, capabilities and status
- 40 SCAP validated products from 30 product vendors
- 9 National Voluntary Laboratory Accreditation Program (NVLAP) Accredited Independent SCAP Testing Laboratories

# NVD Future Capabilities

---

- Create a CCE analysis and scoring capability based on the Common Configuration Scoring System (CCSS)
- Design, build and implement web services that handle requests for NVD SCAP data products.
- Develop and deploy web services & interactive web portal that will streamline and expedite the NCP checklist submission process and help ensure the completeness of submission packages

# Questions?

---

## Contact Info

Christopher Johnson

Computer Security Division

Information Technology Laboratory

National Institute of Standards and Technology

[christopher.johnson@nist.gov](mailto:christopher.johnson@nist.gov)

(301) 975-5981



National Vulnerability Database

<http://nvd.nist.gov>