

# ***Proactive Network Security: Do You Speak CVE?***



## **CVE® WHITEPAPER**

by Gary S. Miliefsky, CISSP®

December 2004

**PredatorWatch, Inc.**

73 Princeton Street, Suite 309  
N. Chelmsford, MA 01863  
978.251.0823 or 877-677-3328  
[www.predatorwatch.com](http://www.predatorwatch.com)

The CVE Standard – Funded by the U.S. Department of Homeland Security and  
Operated by MITRE Corporation.

CVE and the CVE logo are registered trademarks of The MITRE Corporation.  
Use of the Common Vulnerabilities and Exposures List and the associated  
references from MITRE are subject to the Terms of Use. For more information,  
please visit <http://cve.mitre.org> or email [cve@mitre.org](mailto:cve@mitre.org)



# CONTENTS

INTRODUCTION .....	3
DO YOU SPEAK CVE?.....	4
KEEP UP TO DATE ON CVEs.....	5
IN BUSINESS .....	5
IN GOVERNMENT.....	6
REAL WORLD SCENARIO: ELECTRONIC COMMERCE .....	7
WHAT IS ISO17799? .....	8
REAL WORLD SCENARIO: ONLINE BANKING.....	9
EXPLOITING CVEs .....	10
REMOVING CVEs .....	11
PROTECT AGAINST CVE EXPLOITERS.....	11
DETECT AND TRACK ASSETS .....	12
AUDIT YOUR NETWORK FOR CVEs .....	12
LOCK THE DOORS AGAINST CVE EXPLOITS.....	12
CLEANUP YOUR CVEs.....	12
CREDITS: .....	13
FOR MORE INFORMATION:.....	14



# INTRODUCTION

## PROACTIVELY PROTECT YOUR NETWORK-BASED ASSETS

Organizations of all sizes invest billions of dollars each year on network security technologies. Yet they still continue to fall prey to denial of service attacks, fast moving viruses and blended threats, hackers and worms.

A single enterprise can spend millions per year on IDS, firewalls and anti-virus software, while the real network security culprits – common vulnerabilities and exposures (CVEs) – go largely undetected and uncorrected. CVEs are the systemic cause of over 90% of all network security breaches.

While it's true that managing vulnerabilities is an arduous task and organizations have limited resources, the risks and costs to the enterprise are far greater if these weaknesses are not addressed.



**Figure 1. Behind the Firewall...A Gift From A Friend?**

Today's networks are at risk. Not just because hackers are out there, but also because in a mobile world, any device can pick up a virus or Trojan or have a vulnerability that opens just enough of a window to your network that a hacker can exploit it to gain access. Just one CVE® in your network and you may be in trouble. **CVE is the Standard by which all information security professionals will be judged and the litmus test against regulatory compliance** including GLBA, HIPAA, 21 CFR FDA 11, E-Sign and SO-404 as relates to information assets.



# DO YOU SPEAK CVE?

The most important information security question you need to answer is “Do You Speak **CVE**?” If you do not, then no matter how much you spend on INFOSEC countermeasures, you’ll never fully understand why you are experiencing downtime and successful hacker attacks. Not to mention the regulatory compliance risk you face.

**Common Vulnerabilities and Exposures (CVE)** is a list or dictionary that provides common names for publicly known information security vulnerabilities and exposures. Using a common name makes it easier to share data across separate databases and tools that until now were not easily integrated. This makes CVE the key to information sharing. If a report from one of your security tools incorporates CVE names, you may then quickly and accurately access fix information in one or more separate CVE-compatible databases to remediate the problem.

**CVE – An Industry Standard funded by the Department of Homeland Security – Operated by MITRE.**

**CVE is:**

- One name for one vulnerability or exposure
- One standardized description for each vulnerability or exposure
- A dictionary rather than a database
- How disparate databases and tools can "speak" the same language
- The way to interoperability and better security coverage
- A basis for evaluation among tools and databases
- Accessible for review or download from the Internet
- Industry-endorsed via the CVE Editorial Board

Some CVEs are currently Candidates (CANs) – keep an eye out on both CVEs and CANidate CVEs.

**Example CANDidate CVE:**

CAN-2003-0352 (under review)

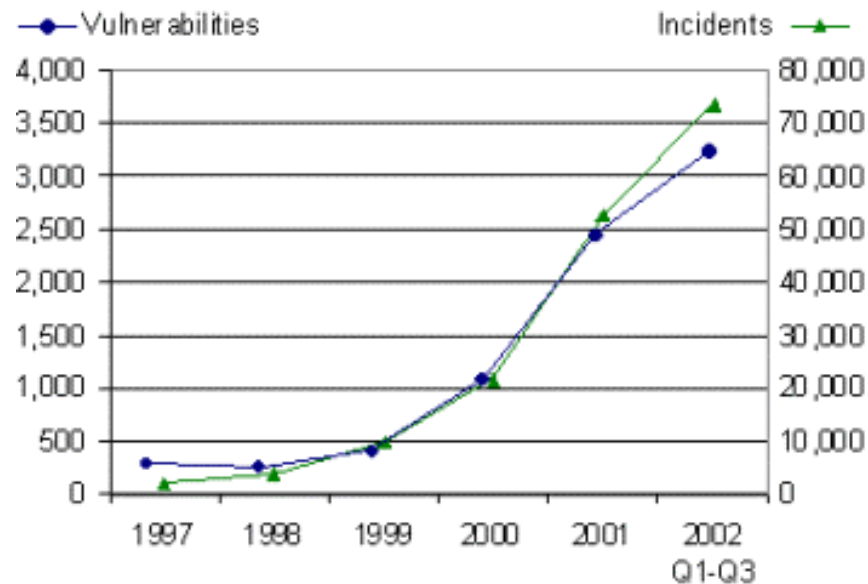
Buffer overflow in a certain DCOM interface for RPC in Microsoft Windows NT 4.0, 2000, XP, and Server 2003 allows remote attackers to execute arbitrary code via a malformed message.

**What exploited this CVE?** Blaster, Msblast, LovSAN and the Nachi and Welchia worms causing massive downtime and financial losses.



# KEEP UP TO DATE ON CVEs

It is impossible today to prevent vulnerabilities across the enterprise. Knowing what they are, where they are on your network, and how to remove them is more important than sniffing packets and listening for burglars.



**Figure 2. CVEs and CVE Exploit Attacks on the Rise**

Take this opportunity to harden your network assets by using the following formula:

1. Visit <http://cve.mitre.org>
2. Keep an eye on the CVEs contained on the SANS/FBI top 20 list <http://www.sans.org/top20/>
3. Test for the latest CVEs on a daily basis
4. Report on your CVEs on a daily, weekly or monthly basis (DUE DILIGENCE)
5. Remove all CVEs that you possibly can (DUE CARE)
6. Block at the Firewall (INCREASE UPTIME)

## ***IN BUSINESS***

Hackers cause over \$2 Billion in damages by using CVEs against us and the damages are growing annually (Source: CSO Magazine). How many CVEs do you have in your Network? Is your computer network taking you out of compliance? Knowing if you have any CVEs is the only way to find out and is considered Due Diligence. Removing critical CVEs is considered Due Care.



Frequent and consistently scheduled security audits for CVEs and their removal is the only prudent thing to do as a proactive information security manager.

## ***IN GOVERNMENT***

**EXECUTIVE ORDER – EO – 13231**...to ensure protection of information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems, in the information age.

**HB 2211 FOIA**; critical infrastructure and vulnerability assessments.

**NIST** recommends that Federal departments and agencies ...

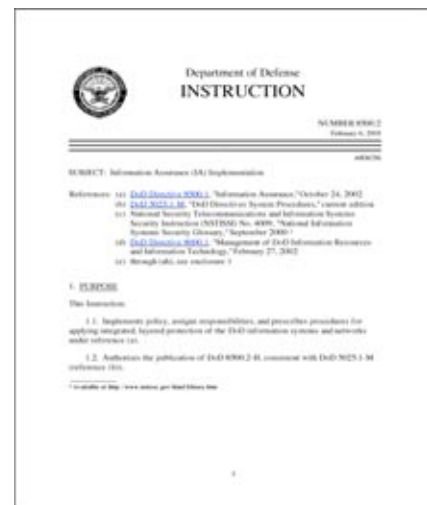
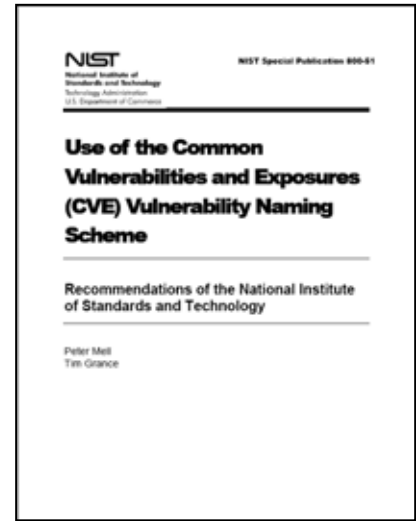
- *Give substantial consideration to acquisition and use of security-related IT products and services compatible with the CVE naming scheme.*
- *Periodically monitor systems for applicable vulnerabilities listed in the CVE naming scheme.*
- *Use CVE vulnerability naming scheme in descriptions/communication of vulnerabilities.*

The following appears for all three Mission Assurance Categories of DoD systems in DoD Instruction 8500.2:

### **DoD Guidelines for Vulnerability Management:**

A comprehensive vulnerability management process ... automated vulnerability assessment or state management tools ... regular internal and external assessments are conducted ... For improved interoperability, preference is given to tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention...to test for the presence of vulnerabilities.

With growing risk of legal liability, regulatory compliance, constant watch and protection of intangible computer-based assets, a vigilant proactive approach to network security is a requirement in today's network economy. Knowing which systems have CVEs





and how to mitigate risk against those CVEs should be a top priority of U.S. Government IT managers.

## REAL WORLD SCENARIO: ELECTRONIC COMMERCE

What if you were the CEO, CFO, CIO or CSO of an E-commerce Merchant or a Brick & Mortar Retailer using an Internet Payment Gateway System? What if you had only one CVE in your system? What if anyone could exploit it in 5 minutes?

VISA announced vulnerability audit requirements called the VISA CISP program. Over 21,000-member financial institutions, VisaNet processes over 2,700 transactions/sec during peak season.

MasterCard requires Quarterly Audits beginning 6/2004 in the MasterCard SDP program. 7% of all of MasterCard's \$921.6 billion annual card purchases take place on the web. To understand where CVEs fit into this best practices model for information security in electronic commerce, see page 49 of MasterCard SDP PDF, currently found at:

[https://sdp.mastercardintl.com/pdf/Standards\\_Applicable\\_To\\_Vendors.pdf](https://sdp.mastercardintl.com/pdf/Standards_Applicable_To_Vendors.pdf)

American Express has launched the DSS program and Discover Card has launched the DISC program. Soon, all e-Commerce Merchants must detect/remove critical CVEs to do business online.

All of these information security programs require security policies in place and audits on a regular basis. So, what should you do to comply?

1. Build Corporate Security Policies that are ISO17799 compliant.
2. Audit your entire network including your web server for CVEs.
3. Report on those CVEs that you're finding and removing.

You're probably wondering what is ISO17799? In summary, it's a best practices policy model that is accepted as an international standard. You'll find CVE® auditing requirements in each credit card provider program, from VISA CISP to MasterCard SCP. Policies and processes must be in place so that you can show a paper trail for due diligence and due care to report on your best practices to the electronic commerce provider. The ISO17799 model is the best way to do it.

Now that you know what CVEs are, let's explore the ISO1779 model.



# WHAT IS ISO17799?

The ISO17799 model for information security comes from the International Organization for Standardization (ISO).

ISO is a network of national standards institutes from 146 countries working in partnership with international organizations, governments, industry, business and consumer representatives. ISO also serves as a bridge between public and private sectors. You can learn more about ISO at <http://www.iso.org>.

The ISO17799 standard contains ten sections:

1. **Security Policy** – To provide management direction and support for information security
2. **Organizational Security** – To manage information security within the organization
3. **Asset Classification and Control** – To maintain proper classification and protection of organizational assets
4. **Personnel Security** – To reduce the risk of human error, theft, fraud or misuse of your company or organization
5. **Physical and Environmental Security** – To prevent unauthorized access, damage and interference to business premises and information
6. **Communications and Operations Management** – To ensure the correct and secure operations of information processing
7. **Access Control** – To control access to information
8. **System Development and Maintenance** – To ensure security is built into information systems development and maintenance processes
9. **Business Continuity Management** – To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters otherwise known as BCP/DRP
10. **Compliance** – To avoid breaches of any criminal and civil law, statutory, regulatory or contractual within your business model and government guidelines

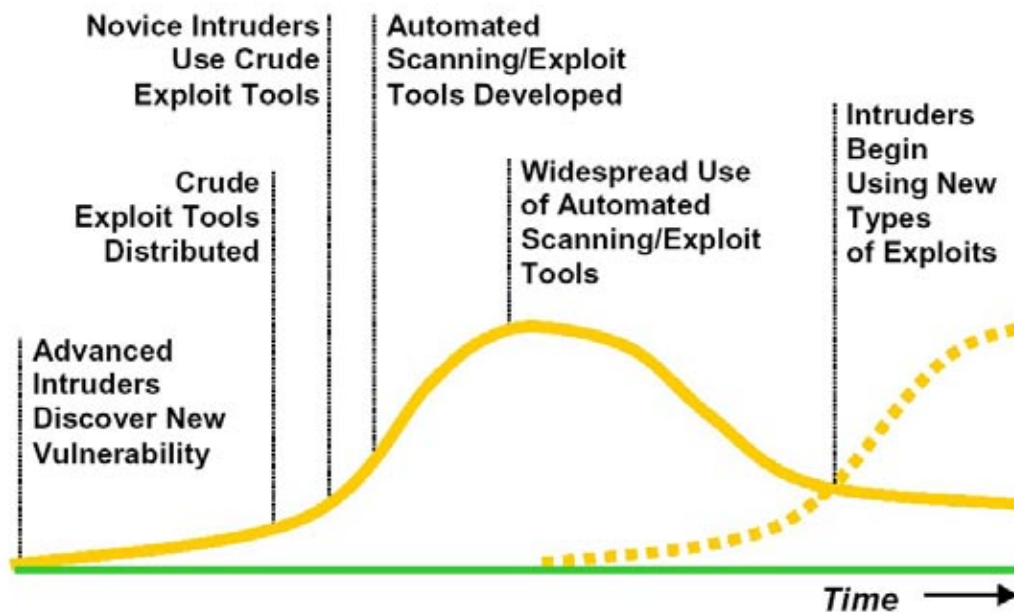


# REAL WORLD SCENARIO: ONLINE BANKING

What if you were the CEO, CFO, CIO or CSO of Fidelity Trust Bank with \$1B under management? What if you had only one CVE in your system? What if anyone could exploit it in 5 minutes?

A special investigator on the Task Force on the Investigation of Internet states "someone who knows a system could hack it by sneaking in a back door."

This is known as *Exploiting a CVE*. **Hackers and their automated tools are CVE Exploiters.**



**Figure 3. CVE Exploiters use the Window of Vulnerability**

Per CNN, which documented an online bank heist, "even if you have never banked online, your money may never be completely safe from an electronic heist. Nearly every bank in the United States runs its operations on an internal network that connects to the Internet at some point. Although the banking industry claims that its security is virtually foolproof, others say that any technology can be penetrated under the right circumstances."

By now you should realize how important it is to speak CVE. You should also consider that the daily removal of high-risk CVEs may protect you from hackers, downtime and regulators.



In seizing control of a server, security experts say, a hacker can also modify any trusted applications to perform malicious operations. An attack that manipulates such internal applications is more likely to escape notice by the network's electronic guards.

"Intrusion-detection systems only spot known attacks or behaviors that indicate a certain class of attack," said the expert. "Attacks against a server might be detected, but a complex application-based attack might look like normal behavior."

Financial institutions do make it difficult for employees to move money, but their systems must be flexible enough to work with customers who are not subject to the same level of scrutiny. This could allow an insider to create a fake customer transaction and authorization to shepherd the money right out of a system."  
(Source: CNET News.com)

## EXPLOITING CVEs

All hackers and the automated tools they have created use the same methodology. The amount of damage they may cause depends on how far they or their tool goes and the CVEs they find and exploit:

1. Footprint your servers, desktops and network infrastructure.
2. Scan for numbers of computers, open ports, services running.
3. Enumerate those servers and services they can find.
4. Penetrate those systems that have high-risk CVEs.
5. Escalate their privileges to become a super-user or administrator.
6. Pillage your information and customer records.
7. Get interactive including installing helper software to let them in later.
8. Expand influence by replacing trusted programs with backdoors.
9. Cleanup their tracks including firewall and server logs.

And if they want to disrupt your business, they will perform:

10. DoS (Denial of Service) attacks against you or others, using your resources.

Sometimes they install software known as Zombies, which are used as remotely controlled or preconfigured DoS attacking tools that use your resources against another target, such as another online bank.



## REMOVING CVEs

CVE Management is the key to hardening your network assets. Three types of solutions that claim to help you harden your assets are:

1. Configuration Management
2. Patch Management
3. Vulnerability Management

If you find a solution that helps automates this process for you, make sure it helps find and fix CVEs. If the solution you choose has not been vetted by MITRE, then it may not be compatible with the CVE standard.

Look for this logo:



to accompany the product or service in question – verify it at <http://cve.mitre.org>.

Every day there is a new CVE so keep an eye on <http://cve.mitre.org>. As you now know, this website is the homepage for helping you stop hackers and harden your assets. Why? By knowing the CVEs, if you find a system with a CVE, then you can find a way to block an exploit that would impact this asset.

## PROTECT AGAINST CVE EXPLOITERS

There are four key things you can do to protect yourself against CVE Exploiters:

1. **Detect and Track Assets**
2. **Audit your Network for CVEs**
3. **Lock The Doors against CVE Exploits**
4. **Cleanup your CVEs**



## ***DETECT AND TRACK ASSETS***

Do you have policies and systems in place to track all of your network-based assets? Do you allow laptops in and out of the office? Are laptops a company asset or a personal computer that can be used at home? Do you require firewall, antivirus, antispysware and patches to be installed on each host and up to date? What about wireless routers and ad-hoc wireless LANs – have you sniffed the airwaves and port connections to see if there are any new wireless devices or servers connected to your network? Answering these questions is critical in the protection of these assets against CVE exploiters.

## ***AUDIT YOUR NETWORK FOR CVEs***

Find a tool you like. Google “Laptop Auditor” or “Security Auditor” or use similar keywords and you’ll find companies and products in this marketplace. Do an evaluation of open source versus commercial products. If you built your firewall from scratch – go for open source, otherwise find a company you can work with and trust. Make sure to pick a tool that doesn’t take any assets offline and scans and reports on CVEs.

## ***LOCK THE DOORS AGAINST CVE EXPLOITS***

Your firewall is your best countermeasure. Make sure to review logs – look for suspicious traffic. Also make sure you setup the VPN interface properly and know who’s using it and if they are coming in through a secure tunnel on an insecure or ‘sick’ computer. By reconfiguring your rules table around CVE Exploits, you might be one step ahead of the hackers. For example, why not block ports for all inbound/outbound traffic that you don’t use – 445 was exploited by MSBlast and Sasser. Do you need to keep this port open at the firewall? Look at the computers that have CVEs – how long to fix and what port is it on? Update your rules table until it is fixed. Don’t trust all patches. Reinspect for same or new CVEs and the affected ports and services. Keep repeating this process, daily.

## ***CLEANUP YOUR CVEs***

Does your vendor offer patches? Did the patch fix the CVE? Yes, good. No? Then, why not shut off the service or feature that harbors the CVE – one quick configuration change and no CVE to exploit. Some CVEs can be patched while others require intelligent reconfiguration. Cleanup your CVEs on the most important systems and highest risk of attack. Keep repeating this process, daily.



## CREDITS:

Thanks to numerous PredatorWatch, Inc. customers for their time in reviewing this document and suggestions.

Many thanks to the MITRE CVE team, <http://cve.mitre.org>, for their work in creating and standardizing CVEs.

CVE® and the CVE logo are registered trademarks of The MITRE Corporation. Use of the Common Vulnerabilities and Exposures List and the associated references from MITRE are subject to the Terms of Use.

For more information, please email [cve@mitre.org](mailto:cve@mitre.org)



CVE® is sponsored by U.S. Department of Homeland Security.  
For more information, please visit <http://www.us-cert.gov>



## FOR MORE INFORMATION:

email inquiries to: [cve@predatorwatch.com](mailto:cve@predatorwatch.com)



**PredatorWatch, Inc.**  
73 Princeton Street, Suite 309  
N. Chelmsford, MA 01863  
978.251.0823 or 877-677-3328  
[www.predatorwatch.com](http://www.predatorwatch.com)