

INNOV-04

# The SANS Top 20 Internet Security Vulnerabilities

(and what it means to OpenEdge™ Applications)

Michael Solomon, CISSP PMP CISM

Solomon Consulting Inc.

[www.solomonconsulting.com](http://www.solomonconsulting.com)

(Thanks to John Bruggeman for presentation input)



PROGRESS SOFTWARE  
**Exchange**  
2005




# What is the SANS Top 20

- ◆ SANS and FBI / NIPC created list in 2000
- ◆ 10 Windows vulnerabilities
- ◆ 10 Unix vulnerabilities
  - 90% of all computer security breaches are caused by known vulnerabilities (Gartner Group 2002)
- ◆ Tools to detect and repair the Top 20
  - Many referenced tools help detect and repair many more than the Top 20 Vulnerabilities



## How do these vulnerabilities affect OpenEdge applications?

- ◆ OpenEdge is not specifically mentioned
  - Many vulnerabilities on the list still apply to OpenEdge application systems
  - Interpret each vulnerability in terms of your system
- ◆ Any system vulnerability affects your OpenEdge application



# Windows Top 10 — [www.sans.org/top20/#w1](http://www.sans.org/top20/#w1)

1. Web Servers and Services
2. Workstation Service
3. Windows Remote Access Services (not RAS)
4. Microsoft SQL Server
5. Windows Authentication
6. Web Browsers
7. File-Sharing Applications
8. LSAS Exposures
9. Mail Client
10. Instant Messaging



# W1: Web Servers and Services

- ◆ Risks of default installations
  - Denial of service (DoS)
  - Compromise server and data
  - Execution of arbitrary commands
- ◆ All web servers are affected, including
  - Internet Information Server (IIS)
    - Even though IIS 6.0 is ‘secure by default’
  - Apache
  - iPlanet (now SunOne)



# W1: Web Servers and Services

- ◆ If you are running a default installation, you are vulnerable
  - The SANS Top 20 list contains links to several tools
- ◆ How to protect against these vulnerabilities
  - Patch your software!
  - Remove unused scripts, binaries and accounts
  - Remove or restrict common attack targets
    - tftp, ftp, cmd.exe, bash, net.exe, remote.exe, telnet
- ◆ OpenEdge impact – any application component that allows access from the web



## W2: Workstation Service

- ◆ Processes user requests to access resources such as files and printers
  - Service contains a stack buffer overflow
- ◆ Operating systems affected
  - Windows 2000 (SP2, SP3 and SP4)
  - Windows XP SP1 & 64 bit edition
- ◆ How to protect your system
  - Patch your software!
  - Windows XP SP2 (Win 2000 – MS03-049)
  - Block ports 139 & 445 from outside
- ◆ OpenEdge impact – any systems that share resources in your DB/AppServer™ environment



## W3: Remote Access Services

- ◆ Risks - Compromised host or data, DoS
- ◆ All Windows OS's are affected
- ◆ Examples
  - Windows file sharing
    - NETBIOS shares (C\$)
  - Anonymous Logon (Null sessions)
  - Remote Registry Access
  - Remote Procedure Calls (RPC)



## W3: Remote Access Services

- ◆ How to determine if you are vulnerable
  - SANS Top 20 document links
  - Anonymous Logon
    - C:\>net use \\ipaddress\ipc\$ "" /user:""
    - If “The command completed successfully” displays, you are potentially vulnerable
- ◆ How to mitigate
  - Patch your software!
  - Limit file sharing; never over the Internet
  - No unauthenticated shares
  - Set registry to restrict remote access



## W4: MS SQL Server

- ◆ Risks - Compromised host and data, DoS
- ◆ All Microsoft OS's and SQL versions
- ◆ Even though this is a SQL Server item, OpenEdge users should pay attention to the nature of the vulnerabilities
  - Make sure the same vulnerabilities do not exist on your OpenEdge system
  - SQL Server is on this list due to market share, not that it is more vulnerable



## W4: MS SQL Server

- ◆ The MS SQL vulnerability caused
  - SQL Snake / Spida Worm (May 2002)
    - Default password set to null – default install
  - SQL-Slammer/SQL-Hell/Sapphire worm (Jan 2003)
    - Buffer overflow error
  - SQL MSDE Desktop Engine
    - Can be installed by
      - Office XP, Visual Studio .NET, ASP.NET Web Matrix Tool, Visual Fox Pro 7.0 / 8.0



## W4: MS SQL Server

- ◆ How to protect your system
  - Patch your software!
  - Disable listening on port 1434
    - OpenEdge systems – Do not use default ports
  - Enable SQL authentication logging
    - Accomplished via Enterprise Manager
  - Secure the system (server and network level)
    - Change the default (null or blank) password



## W5: Windows Authentication

- ◆ Password vulnerabilities
  - Weak passwords
  - Unprotected passwords
  - Default system passwords
  - Well known hash algorithms allow easy cracking
- ◆ Risks - Compromised host and data, DoS



## W5: Windows Authentication

- ◆ Windows Hash algorithm problems
  - Windows NT, 2000, XP store LAN Manager (LM) passwords for compatibility
    - LM password hash is very weak
    - Long passwords are truncated to 14 characters
    - Short passwords are padded to 14 characters
    - Passwords are stored all upper case
    - Passwords are broken into 2 7 character blocks



## W5: Windows Authentication

- ◆ Windows LM hash
  - Stored in the SAM database
  - Frequently transmitted over network
    - Hash can be sniffed and cracked
  - The hash can be brute force cracked in a few days
- ◆ All Microsoft OS's are affected
- ◆ How to mitigate
  - Good Password policy
    - Enforce strong passwords
      - Special characters,
    - Enforce password aging, length, minimum age



## W6: Web Browsers

### ◆ Risks - Dozens of vulnerabilities

- Cross-site Scripting
- Poor security in ActiveX modules
- MIME types not correctly identified
- Standard buffer overflow
- Spyware/Adware vulnerabilities

### ◆ Not just IE anymore

- IE
- Mozilla
- Firefox
- Netscape
- Opera



## W6: Web Browsers

- ◆ All OS and versions are affected
  - IE installed on almost all Windows machines due to tight integration into the OS
  - Vulnerabilities exist even if you don't browse the web
- ◆ How to determine if you are vulnerable
  - Unless you are fully patched, you are vulnerable
- ◆ How to protect
  - Patch your software!
  - Modify default Internet security
    - Internet Options -> Tools -> Security tab
      - Set to prompt for Active Scripting
      - Disable ActiveX
      - Annoying but significantly more secure



## W7: File-Sharing Applications

- ◆ Peer to peer (P2P) applications
  - Popular to download and distribute many types of data
- ◆ Risks - Possible compromised host, spyware, legal liability
- ◆ All Windows platforms are affected
- ◆ How to determine if you are at risk
  - If you have installed P2P software you may be vulnerable



# W7: File-Sharing Applications

- ◆ How to protect against it
  - Establish a P2P policy against downloading copyrighted materials
  - Monitor usual ports
    - Napster TCP 8888, 8875, 6699
    - eDonkey TCP 4661, 4662, UDP 4665
    - Gnutella TCP/UDP 6345, 6346, 6347, 6348, 6349
    - Kazaa WWW (TCP 80), TCP/UDP 1214



## W8: Local Authority Subsystem Service (LSAS) Exposures

- ◆ Important in System authentication and Active Directory
- ◆ Contains a buffer overflow vulnerability
  - Exploited by Sasser and Korgo worms
- ◆ Affected OS's
  - Windows 2000
  - Windows XP & 64 bit edition
  - Windows 2003



## W8: Local Authority Subsystem Service (LSAS) Exposures

- ◆ How to protect your system
  - Patch your software!
  - Block the following ports:
    - UDP/135, UDP/137, UDP/138, UDP/445
    - TCP/135, TCP/139, TCP/445, TCP/593
  - Ensure your firewall is properly configured



## W9: Mail Client

- ◆ Risks - Allows attackers to run the code of choice on a machine
- ◆ All Microsoft OS's are affected
- ◆ If mail client is loaded you are vulnerable
- ◆ How to protect your system
  - Patch your software!
  - Disable Message Preview panel
  - Block suspicious attachments
  - Remove unused mail clients



## W10: Instant Messaging

- ◆ IM has seen tremendous growth and maturity
- ◆ Risks – data disclosure or modification, loss of productivity
- ◆ All Microsoft OS's are affected
- ◆ How to protect your system
  - Patch your software!
  - Configure your firewall to disallow IM file transfers
  - Block access to web pages containing links such as “aim:” or “ymsgr:”



# Unix Top 10 - [www.sans.org/top20/#u1](http://www.sans.org/top20/#u1)

1. BIND Domain Name System
2. Web Server
3. General Unix Authentication (Weak passwords)
4. Version Control Systems
5. Mail Transport Service
6. Simple Network Management Protocol (SNMP)
7. Open Secure Sockets Layer (SSL)
8. Misconfiguration of Enterprise Services (NIS/NFS)
9. Databases
10. Kernel



# U1: BIND Domain Name System

- ◆ Risks - Loss of Internet naming system, DoS
- ◆ Nearly all Unix and Linux flavors are affected
- ◆ How to determine if you are affected
  - Type “`named -v`” to see what version you are running
- ◆ How to protect against vulnerabilities
  - Patch your software!
  - Disable *named* unless DNS is required
  - Change version information in the `named.conf` file
  - Run BIND from a non-privileged account



## U2: Web Server

- ◆ Risks - DoS, information disclosure, remote root access
- ◆ All Linux and Unix flavors can run a web server
- ◆ Most common UNIX/Linux web servers (and add-on modules)
  - Apache
  - iPlanet/Sun Java System
  - PHP
  - OpenSSL
- ◆ All un-patched software is vulnerable



## U2: Web Server

- ◆ How to protect against vulnerabilities
  - Patch your software!
  - Don't run as root
  - Limit server information
- ◆ OpenEdge users - pay attention to web-related vulnerabilities
  - Web servers provide critical front-end access to many OpenEdge applications



## U3: Authentication

- ◆ Risks - compromised host and data, DoS
- ◆ All UNIX/Linux systems are affected
- ◆ How to determine if you are vulnerable
  - Look for generic accounts
  - Check etc/passwd with a password checker
  - Search for clear text transmission of passwords
    - Telnet, FTP, HTTP, DB connection
- ◆ How to mitigate
  - Same strong password policy as Windows



## U4: Version Control Systems

- ◆ Version control systems manage changes to documents or source code
  - The most popular, CVS and Subversion, both contain heap-buffer overflow vulnerabilities
  - Can allow remote execution of arbitrary code
- ◆ Risks – compromised host, ability for attacker to execute arbitrary code
- ◆ All Linux/UNIX systems that run version control systems are vulnerable



## U4: Version Control Systems

- ◆ How to determine if you are vulnerable
  - Check CVS version “cvs ver”
    - stable rel ver 1.11.16 and prior, feature rel ver 1.12.8 and prior
  - Subversion prior to 1.0.5 configured for remote access
- ◆ How to mitigate
  - Patch your software!
  - Use SSH instead of pserver protocol (CVS)
  - Use webDAV instead of svn protocol (Subversion)
  - Block ports if repository access is internal only
    - CVS – 2401/tcp
    - Subversion – 3690/tcp



## U5: Mail Transport Service

- ◆ Risks - Privilege escalation, open relay
- ◆ All Linux/UNIX systems are affected
- ◆ How to determine if you are vulnerable
  - Outdated or un-patched mail transport agents are vulnerable
  - Refer to SANS Top 20 list for more details:
    - Sendmail
    - Exim
    - Qmail
    - Courier-MTA
    - Postfix
  - Assess your mail server using a vulnerability scanner



## U5: Mail Transport Service

- ◆ How to protect your system
  - Patch your software!
  - Disable mail transport services on systems not designed to be mail servers
- ◆ Verify configuration will not allow relay of email
  - Consult SANS Top 20 list for specifics



## U6: Simple Network Management Protocol (SNMP)

- ◆ Risks - Compromised host, privilege escalation
- ◆ Nearly all Linux/UNIX systems come with SNMP and are vulnerable
  - Many have SNMP installed and active by default
- ◆ Scan your network to see if you are vulnerable
- ◆ How to protect your system
  - Patch your software!
  - Disable SNMP unless needed
  - Filter SNMP traffic (161 tcp/udp, 162 tcp/udp)
  - Modify community strings



## U7: Open Secure Sockets Layer (SSL)

- ◆ Risks - Remote code execution, root privilege escalation
- ◆ Nearly all UNIX/Linux flavors can run Open SSL
- ◆ How to determine if you are vulnerable
  - Check your version – “openssl version”
    - Version 0.9.7c or earlier is vulnerable
- ◆ How to protect your system
  - Patch your software!
  - Use IP filtering to limit who can access via Open SSL



## U8: Misconfiguration of Enterprise Services (NIS NFS)

- ◆ Risks - Compromised hosts, escalated privileges
- ◆ Most UNIX/Linux flavors run NIS and NFS
- ◆ How to determine if you are vulnerable
  - Check version to verify on the most recent version
- ◆ How to protect your system
  - Configure client to only connect to specific NIS server
  - For NFS – use numeric IP addresses not aliases
  - Check NFS configuration with NFSBug
  - Use /etc/exports to restrict access to NFS



## U9: Databases

- ◆ Databases are the core component in most business applications
- ◆ Risks – data integrity, confidentiality, and availability
  - Databases provide attractive targets for attackers wishing to access restricted data
- ◆ OpenEdge users should pay particular attention to database vulnerabilities
  - Even though well-known database port lists generally do NOT include Progress and OpenEdge dbs, a quick visit to [www.progress.com](http://www.progress.com) provide attackers with all the information they need for default ports.



## U9: Databases

- ◆ How to determine if you are vulnerable
  - If you use a DB product, you are
- ◆ How to protect your system
  - Patch your software!
  - Know the risks
  - Harden your database and software
    - This is the hardest part
    - See the references section for more information



# U10: Kernel

- ◆ Core OS functionality
  - The kernel manages interaction between OS and hardware
  - Often operates in privileged mode
  - A kernel compromise can be devastating
- ◆ All systems are vulnerable (even Windows)
- ◆ How to protect your system
  - Patch your kernel!
  - Use a vulnerability scanner to assess your systems
  - Harden your kernel



# Summary

- ◆ Use the SANS Top 20 list as a guideline
- ◆ Although OpenEdge is not on the list, many vulnerabilities still apply to your applications
- ◆ Good security requires frequent attention
- ◆ Take the time to learn how to harden your systems, then do it!



# Resources

- ◆ Solomon Consulting Inc.
  - [www.solomonconsulting.com](http://www.solomonconsulting.com)
- ◆ SANS Top 20 list
  - [www.sans.org/top20](http://www.sans.org/top20)
- ◆ Website that tracks top scanned ports
  - [www.incidents.org](http://www.incidents.org)
- ◆ Lists of MS bugs, patches, and security updates
  - [www.microsoft.com/technet](http://www.microsoft.com/technet)
  - [www.ntbugtraq.com](http://www.ntbugtraq.com)
- ◆ Great site for latest vulnerabilities
  - [www.insecure.org](http://www.insecure.org)