

TrustKeeper®

A product of  Trustwave®

Full Vulnerability Scan

DTT Surveillance Inc







Dec 10, 2008

CONTENTS





Report Overview.	1
Security Compliance Dashboard.	2
Scan Parameters.	3
Discovered Systems.	4
Scanning Results and Recommended Actions.	5
Vulnerabilities Fundamentals.	5
Vulnerability Scoring.	7
Vulnerabilities By Device.	8
Appealing Report Findings.	9
System Information.	10
Inventory.	11
Accessible Web Servers.	12
Resources: Improving Your Company's Security.	13

ICON OVERVIEW

The following icons are used throughout the report to identify the severity and compliance-affecting nature of the findings presented in the report.

Icon	Name	Description
	Compromised	Compromised events indicate there is evidence that a system has previously been successfully attacked. You should investigate and validate these issues immediately. (PCI Level 4 and 5 vulnerabilities are included here)
	High Severity	High Severity vulnerabilities indicate problems which could result in immediate compromise. These issues should be investigated and validated as soon as possible in order to reduce the risk of a successful attack. (PCI Level 3 and 4 vulnerabilities are included here)
	Medium Severity	Medium Severity vulnerabilities indicate issues which could potentially result in information or system compromise. (PCI Level 2 vulnerabilities are included here)
	Low Severity	Low Severity vulnerabilities indicate low risk problems or warnings, such as configurations which might reveal interesting reconnaissance information that could be used to facilitate a compromise (e.g., application "banners"). (PCI Level 1 vulnerabilities are included here)
	Informational	Details about your systems that might be of interest but that do not represent a security threat are indicated by Informational events
	Pass	This icon indicates that the item has passed a security scan.

COMPLIANCE DASHBOARD

Network Scan Vulnerabilities		
	0 High Vulnerabilities	You do not have any high-severity security vulnerabilities in the systems included in your scan.
	1 Medium Vulnerability	You have 1 medium-severity security vulnerabilitie(s) in your systems. Although not an immediate problem, you should begin to develop a remediation plan for these items.
	0 Low Vulnerabilities	You do not have any low-severity security vulnerabilities in the systems included in your scan.
	1 Informational Vulnerability	You have 1 informational notices for your systems.

SCAN PARAMETERS

This section provides details on the scan that was completed on your network. The vulnerability scan is conducted using parameters which describe the subject IP addresses. These parameters include specific IP addresses, blocks of IP addresses and domain names. Domain names are resolved to one or more IP addresses using an enhanced DNS query that allows the scanner to identify multiple servers if certain types of load balancing are used in your network.

Scan Completed On: 2008-12-10 03:38:34.473661 GMT

Network blocks are described using Classless Interdomain Routing (CIDR) notation. Individual IP addresses are notated with a "/32" CIDR suffix.

The following parameters were used as input to this scan:

Scan Parameters		
# -1	Type	Parameter
1.	IP Address	Device 1

RELATED HOSTS (NOT SCANNED)

The following systems were discovered to be related to your network during this scan. TrustKeeper only scans those systems which are explicitly identified by you; however, the following systems were identified using reconnaissance techniques based on the information you provided. While not scanned for this assessment, you should be aware that an attacker could identify the same information.

Please review this information and update your TrustKeeper Scan Parameters if any of the following systems are relevant to the assessment being performed. In many cases, some of these systems will not be relevant to the assessment. Common examples include domain name servers (DNS) and mail servers maintained by your ISP. The scanner may also identify internal systems that are not directly accessible from the Internet.

SCANNING RESULTS AND RECOMMENDED ACTIONS

Common Vulnerabilities and Exposures (CVE)

TrustKeeper utilizes the industry-standard CVE Identifiers as the primary reference for vulnerability findings. CVE Identifiers provide references to the official CVE database maintained by MITRE, as well as the National Vulnerability Database (NVD). CVE Identifiers are included, with links to both the CVE database and the NVD, in the "Description" column of the findings tables included in this report. You may search for specific CVE references in the report using the native search function of your PDF viewer.

Vulnerabilities Fundamentals

Vulnerabilities vs. Exploits

The terms "vulnerability" and "exploit" are used throughout this report. A vulnerability represents a threat to your systems and information. It may be a technical threat, such as a program which contains potential buffer overflows, or it may be a configuration, such as leaving certain network services exposed to the Internet, or not requiring authentication to access a certain feature of a program (e.g., remote authoring with Microsoft FrontPage).

An exploit is a program (e.g., a worm, virus, trojan horse, buffer overflow, etc.) or procedure which actually takes advantage of a vulnerability. An example of a well-known exploit is the Blaster/LovSAN worm which takes advantage of a buffer overflow vulnerability in Microsoft's networking software. The time window between the announcement of a vulnerability and the release of a software patch or upgrade to fix the vulnerability is a critical period in the life of an exploit. Unfortunately, exploits for new vulnerabilities have been appearing faster, increasing the need for system and network administrators to maintain vigilance in their patching and configuration procedures.

Exploit Impact

Successful exploits can result in numerous consequences to your network. A denial-of-service (DoS) may be accomplished by either crashing a server (the system or a particular service) or consuming all or most of a system resource (e.g., bandwidth on your Internet connection, memory or CPU on your server, and number of allowed network connections). Information theft, loss or corruption may result if an attacker is able to read or write files on a system. If these files contain configuration information (e.g., a list of allowed users) additional attacks may be enabled. Many exploits can also result in arbitrary code execution. This means that an attacker will be able to upload his own code to your system and run it, often times with the privileges of the Administrator or "root" user. It is at this point that an attacker can be said to "own your system."

Network Vulnerabilities

A major class of vulnerabilities occurs at the network layer. Fortunately, these are relatively easy to address by common filtering or access control devices, such as firewalls or router access control lists (ACL's). As a general rule, *only those services which **must** be offered to the public should be exposed to the Internet.* Common examples of services you probably want to offer to the public include Web, mail and DNS. Many systems are compromised because the network they are in does not properly restrict incoming network traffic. For example, Microsoft networking protocols (NetBIOS over TCP, RPC, etc.) should *not* be exposed to the Internet, as they are intended to offer file and printer sharing, as well as network browsing, on a local network. Also, databases (e.g., Microsoft SQL Server, Oracle, Sybase, MySQL, PostgreSQL, etc.) which contain sensitive information should never be directly exposed to the Internet. Similarly, monitoring and management protocols such as SNMP and Telnet should not be accessible to the general public. Firewalls and routers can be configured to allow restricted access to select users when remote connections to these kinds of protocols are required.

Service Vulnerabilities

A large number of vulnerabilities have been discovered (and exploited) in common software packages, especially Web, mail and database servers. Most of these involve **buffer overflows**. While buffer overflows can be a complex and technical subject to discuss in detail, they can generally be understood as problems involving the processing of user-provided data, such as a user name, password, account number, etc.. Buffer overflows are particularly concerned with malicious users sending an unusually large amount of data

(e.g., a 500 character password or filename) that the application or program was not expecting. In many cases, the "extra" data provided by the user is a small program that the vulnerable system will end up running, often at a high privilege level (e.g., as the "root" or "Administrator" user).

This report reflects the results of a scan that does not intentionally use destructive tests. For that reason, the scanner places significant emphasis on determining the versions of applications that are being used on your systems. If the scanner obtains misleading or inaccurate version information from a network service, it is possible that a vulnerability will either be missed or falsely reported.

Important Notes Regarding Upgrades and Patches

The general solution to service level vulnerabilities is to either update the suspect software package with a patch or upgrade provided by the vendor, or to reconfigure the service. One of the biggest concerns in the day-to-day activities of a system administrator is that all network services (Web, mail, DNS, database, etc.) are up-to-date with security patches and are properly configured. This is especially important on systems and services which are exposed to the Internet. *Administrators must take care to ensure that a new patch or version they intend to install will not "break" an existing business application due to some incompatibility with other software.*

It is a good practice to carefully plan upgrades and to maintain at least a small test environment so that updates to critical services can be tested before being introduced to a production server.

This report provides links to sites which are the principal source of patches and upgrades; however, you should check with the vendor of your system, especially if you are administering a Unix system, to see if they have specific patches for a problem.

Application Vulnerabilities

One of the most serious issues facing many Web sites today is the number of vulnerabilities introduced to the site by custom Web applications which are running on their Web servers. "Web apps" include anything beyond simple, static content on a Web site. Common Web applications include shopping carts and home banking services. Essentially, if a Web site accepts and processes any data from a remote user (e.g., through a form on a Web page), then there is an opportunity for an attacker to take advantage of weaknesses in the code which processes that data. A Web application can be built from popular scripting languages such as Perl and PHP, dynamic HTML technologies such as Microsoft ASP's and Java JSP's, and many other programming languages. Complex Web apps may include Web servers, application servers and dedicated database servers. Common security issues which face Web apps include improper "cleansing" of user-provided data (e.g., does the username you asked for contain too many characters, or include an embedded database query in it) and weak user authentication mechanisms.

SQL Injection & Cross-Site Scripting

Two well known application-level vulnerabilities are "SQL Injection" and "Cross-Site Scripting" (XSS). Both of these types of attacks take advantage of the fact that an application developer has not checked the input provided by users before processing or acting on that input. SQL Injection refers to attempts to send commands directly through to the back-end database used by an application. If successful, such an attack may return content from the database to the attacker, or possibly alter or destroy the data within the database. Cross-site scripting vulnerabilities allow an attacker to trick a web application into returning Javascript (or other executable code) to unsuspecting web browsers, potentially putting that user's data (especially information stored in cookies) at risk.

While it is usually only possible to fully validate these vulnerabilities in a test or QA environment, the TrustKeeper scanner attempts to detect indicators of an application's vulnerability to these two classes of attacks. In both cases, the scanner searches for web forms and embedded links and attempts to submit information which could provoke an error message or other detectable content that would be returned to a web browser. If your report includes such findings, you should review the returned data in any evidence links provided in the report. Obvious error messages, such as "500 Errors," or messages returned with references to "ODBC Errors" or similar sounding problems should be investigated at once. At a minimum, these messages indicate that the application is not handling errors appropriately. In the worst case, such findings may indicate that the application is indeed vulnerable to a SQL Injection or Cross-Site Scripting attack.

Another good way to evaluate these findings is to check your log files. You should review any log files generated by your application in order to see if they indicate that an application error of some kind has occurred around the time of the scan.

VULNERABILITY SCORING

Common Vulnerability Scoring System (CVSS)

Where appropriate, vulnerabilities are assigned a score ranging from 0 to 10, based on the [Common Vulnerability Scoring System, Version 2 \(CVSSv2\)](#). CVSSv2 is the emerging security-industry standard for scoring the severity of vulnerabilities and provides a consistent algorithm for assessing the severity of a vulnerability. TrustKeeper uses the CVSSv2 Base Score, which is comprised of six factors, as follows:

Exploitability:			
AV:	Access Vector	Can the attacker be remote, or does he need local network, physical access, etc. ?	Network, Adjacent, Local Network, Undefined
AC:	Access Complexity	Is the attack easy or hard to perform?	None, Single, Multiple
Au:	Level of Authentication	Are credentials (e.g., username and password) needed to perform the attack?	None, Single, Multiple
Impact of Attack:			
C:	Confidentiality Impact	Can information be read or downloaded (includes both system and business information)?	None, Partial, Complete, Undefined
I:	Integrity Impact	Can information be destroyed or modified?	None, Partial, Complete, Undefined
A:	Availability Impact	Can legitimate users be denied access to information (e.g., denial of service)?	None, Partial, Complete, Undefined

An example of a CVSSv2 Base Vector and Base Score is: AV:N/AC:L/Au:N/C:P/I:N/A:N (Base Score: 5.0)

This vector describes a low-complexity, remote-network based attack that requires no authentication and results in partial information compromise.

Note that TrustKeeper uses the CVSSv2 scores as published by the [National Vulnerability Database \(NVD\)](#) whenever possible. Also, in cases where a finding reflects multiple CVE's, the highest-scoring vector is used to calculate the score.

PCI Scoring



Per the requirements set forth for Approved Scanning Vendors (ASVs's) by the PCI Security Standards Council (PCI SSC), vulnerabilities with a CVSSv2 Base Score greater than 4.0 will cause a component to be non-compliant with the PCI Data Security Standard (DSS). There are several cases identified by the PCI SSC that require special handling:

- Any application-level vulnerabilities related to Cross-Site Scripting or SQL Injection must be considered non-compliant with the PCI DSS, regardless of their CVSSv2 Base Score.
- Any vulnerability that is purely related to denial of service, and does not endanger cardholder information, should not negatively affect a component's compliance with the PCI DSS.

Please note that the new CVSSv2-based scoring system may result in new findings which must be remediated in order to maintain compliance with the PCI DSS.

Vulnerabilities By Device

The scan indicates that vulnerabilities were found in your systems. The table below contains the name, level of severity (compromise, high, medium, low or informational), affected service, description, and a recommended remediation action for each of the vulnerabilities on each system in your network.

Device 1 (device1.static.nextweb.net.)					
# - 2	Severity	Score	Port	Vulnerability	Remediation Action
1.			tcp /8892	<p>VNC Accessible</p> <p>The remote server is running VNC. VNC permits a console to be displayed remotely.</p> <p>Service: -</p>	Disable VNC access from the network by using a firewall, or stop VNC service if not needed.
2.			tcp	<p>TCP/IP Technical Information</p> <p>It was possible to extract details about the randomness of various TCP/IP protocol properties. Randomness in the TCP sequence numbering and the ID field of IP datagrams makes it difficult for attackers to spoof connections to your systems.</p> <p>Evidence: TCP SEQ: Constant; IP ID: Incremental;</p>	It may be difficult to change any of these parameters without obtaining low-level patches from your operation system vendor.

Appealing Report Findings

In some cases, you may find it necessary to submit an appeal of one of the vulnerability findings in the report. The TrustKeeper Appeal Process is an easy-to-use service offered through the TrustKeeper Web site which you may use to request that one or more of the findings be reconsidered or removed from the report.

The TrustKeeper Appeal Process may be useful to you if one of the following circumstances apply:

- You or your hosting center applies upgrades, patches or "back ports" which do not alter the versioning information gathered by the scanner
- You are in a shared environment, such as a hosting center, and you believe that an identified policy violation does not apply to you. For example, an Internet-accessible database may be identified as a policy violation; however, you do not use that database to store any sensitive information.
- You believe that one of the findings is inaccurate.

Please note that if you make changes to your network in order to address a finding (e.g., you install or reconfigure a firewall), you should request a new scan to validate that the changes adequately addressed the relevant issue. Appeals should only be used to make administrative changes to your report in cases where a new scan would not detect any differences.

ACCESSIBLE SYSTEMS AND SERVICES

Reading Your Scan Inventory

The vulnerability scan reveals Internet-accessible hosts and network services available on your network. The following systems (e.g., servers, routers, etc.) and network services (e.g., Web and mail servers) were discovered during the vulnerability scan. As a general rule, all unnecessary network services should be disabled, and all other services should be protected by either firewall rulesets or router access control lists (ACL's). Only those services which must be available to the public should be visible from the Internet.

Pings

Hosts which respond to ICMP "pings" are explicitly identified in the *Device* column. It is generally considered to be good practice to block inbound pings in either router ACL's or firewall rulesets; however, this decision may be affected by network monitoring needs and other considerations.

Names

A system may be known by many names. For example, a server that offers Web and mail services may be known as both *www.mycompany.com* and *mail.mycompany.com*. This report includes as many names as could be identified, including public domain names, Windows domain/workgroups, Windows name, and the "real" name assigned in your DNS server.

Service State

A large number of services (e.g., TCP and UDP ports) are probed during the scan. Ports will either be listed as being *open*, *closed*, or *filtered*, as described below:

- **Open:** The service is "up" and waiting for connections from remote users.
- **Closed:** The service (or a filtering device "in front of" the service) explicitly rejected the connection attempt.
- **Filtered:** There was neither a positive nor negative response. The connection request "timed out," meaning either no service was present, or a filtering device is configured to ignore requests to connect to the port in question.

You should review this list to ensure that only those services you intend to offer to the public are accessible (i.e., "open"). All other "internal" services should be protected using either router access control lists (ACL's) or firewall rulesets.

Inventory

#	Device	ICMP Ping	Possible System Type(s)	Service Information			
				Port	Protocol	Application	Details
1.	Device 1 <i>device1.static.nextweb.net.</i>			tcp/80	http	http	GeoHttpServer
				tcp/8866	generic_tcp	-	D3"\x11\x00\x00\x00\x00\xa5"\x00\x00\xa6"\x00\x0
				tcp/8867	-	-	-
				tcp/8869	generic_tcp	-	\x08 \x00\x0
				tcp/8870	-	-	-
				tcp/8871	-	-	-
				tcp/8888	-	sun-answerbook	-
				tcp/8890	generic_tcp	-	\x00@\x00\x00\x00\x0f\x04\x07\x00\xe0\n\x00\x00@\x00\x00\x00\x00\x00\x00\x00
				tcp/8891	generic_tcp	-	RFB 003.008
				tcp/8892	http	seosload	-
				All other scanned ports were CLOSED			

ACCESSIBLE WEB SERVERS

It is important to pay special attention to the security of your Web servers. This section provides a convenient list of all of the Web servers found in the course of the network scan based on the network parameters you provided in the Network Questionnaire. Information profiled includes the server type (e.g., Microsoft IIS or Apache) and the title of the default Web page. You should ensure that all Web servers listed in this section are authorized and intended to be running in your network since many systems will inadvertently be configured with some type of Web server when they are installed. In addition, many network devices (e.g., routers, switches and print servers) may have Web-based management interfaces of which you may not have been aware. Whenever possible, unused Web interfaces should be disabled or, at a minimum, password protected.

# -2	System IP Address	Domain Name	Port	Server Type	Default Status and Title/Redirect
1.	Device 1		tcp / 80	GeoHttpServer	(200) DTT OnSite v3.2 Login In Redirect to unknown
2.	Device 1		tcp / 8892	-	

RESOURCES: IMPROVING YOUR COMPANY'S SECURITY

The following Internet sites contain valuable information and system patches, which you may find useful to improve your Information Security posture:

- [CERT Coordination Center](#) - The CERT/CC is one of the major reporting centers for vulnerabilities and security incidents. It is a federally funded research and development center, which was created in 1988 in response to the "Morris Worm." The center is operated by Carnegie Mellon University and is a valuable resource for descriptions of security vulnerabilities, information on vendor patches and system configuration guidelines.
- [CVE Database](#) - The Common Vulnerabilities and Exposures (CVE) list provides a set of standardized names for computer vulnerabilities. The web site is hosted by The MITRE Corporation and is funded by the U.S. Government.
- [Microsoft Security](#) - Microsoft Security Advisories
- [Sun Microsystems](#) - Sun Security
- [Red Hat Security](#) - Red Hat Linux Security
- [Cisco Systems](#) - Cisco Security
- [Apache Web Server](#) - Apache Software Foundation provides one of the most popular web servers in the world.
- [OpenSSH](#) - OpenSSH is a popular implementation of the Secure Shell protocol.
- [OpenSSL](#) - OpenSSL is a popular implementation of the Secure Socket Layer protocol.
- [Oracle](#) - Oracle Security
- [MySQL](#) - Popular open-source database, especially in web hosting centers.
- [PHP](#) - Popular web programming language.
- [Trend Micro](#) - Anti-virus vendor and virus information
- [McAfee Security](#) - Anti-virus vendor and virus information