

# STAT® Scanner

## Product Guide



# Introduction to STAT® Scanner

## The Importance of a Healthy Computer

Newspaper headlines contain almost daily reports on companies that have lost substantial time and money from computer downtime due to hacker break-ins and virus infections. These attacks bog down networks, tie up mail servers, and potentially destroy important data. Both types of intrusions take advantage of computers whose “immune system” has weakened over time due to insufficient maintenance. Just as a human body needs regular check-ups to maintain its ability to thwart infections, computers require regular updates to software and security setting modifications to ward off hostile attacks.

The “doctor” in charge of maintaining the health of computer networks is generally a network security administrator or system administrator. Unfortunately, the sheer bulk and frequency of security advisories that software companies produce can easily overwhelm computer security administrators and their staff. Each advisory must be analyzed by security administrators to determine if it applies to software on any computer in the network. The administrator must then apply the corrective action for each advisory, such as locating, downloading and installing the applicable patch or modifying the affected security setting.

Security administrators need a tool that automates the process of scanning network computers for vulnerabilities and identifies the corrective action for deficient computers. The tool must maintain a knowledge base of vulnerabilities that is kept up-to-date with the hectic rate at which advisories are produced. All computer vulnerabilities must be identified on all computers with an indication by the tool of the severity of the vulnerability. A computer network, like a chain, is only as strong as its weakest link. One computer that has a weakened ability to fend off attacks can be compromised by a hostile intrusion and used as a launching platform to attack its peer computers on the network. Only a computer network with a clean bill of health can withstand the onslaught of attacks faced by contemporary networks.

## What is STAT Scanner?

STAT® Scanner is Harris Corporation’s network security tool that scans a computer network, looking for vulnerabilities that provide hostile intruders a way to compromise the system. By pressing a few buttons, the administrator can scan an entire network of computers and assess the vulnerabilities that exist on the network as determined by STAT Scanner’s vulnerability database. STAT Scanner reduces the cost of maintaining network security by providing the administrator with the information to update the configuration or implement the selected corrective action with a single-button solution.

The database of vulnerability assessment information is based on the knowledge of the STAT team of security engineers who have researched security advisories, knowledge base papers, and professional security group articles to provide a single source of vulnerability information. The STAT team of security and application engineers is available to answer questions concerning STAT Scanner and its vulnerability assessments of computer networks.

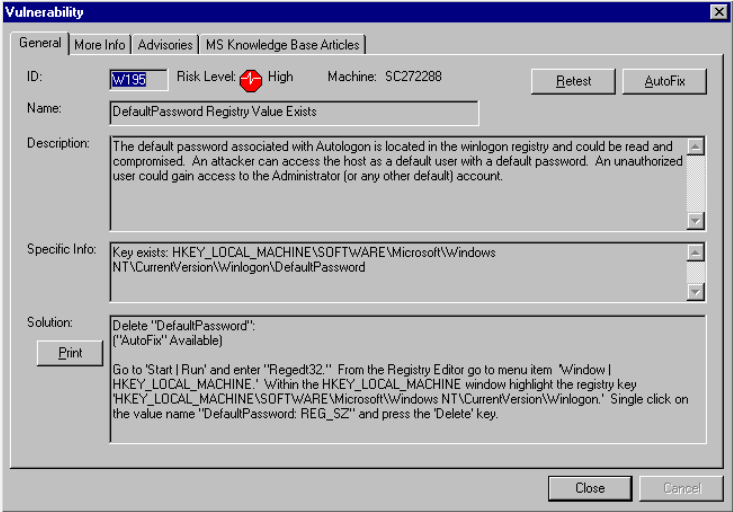
Updates for STAT Scanner are available every month via the STAT website [www.stat.harris.com](http://www.stat.harris.com). These updates keep the network configured with the most current vulnerability information for operating systems as well as third party applications.

## How does STAT Scanner work?

Assessing a computer network with STAT Scanner consists of three easy steps:

1. Discover the computers that exist on the network
2. Scan computers for vulnerabilities
3. Fix the vulnerabilities

## Benefits of STAT Scanner

Feature	Benefit
Easy-to-use Interface	<p>Empowers the administrative organization to implement corrective action based on descriptive information for both the problem and the solution. The “AutoFix” button provides a single button press solution for many vulnerabilities. “Batch AutoFix” applies the corrective action to multiple computers.</p>  <p>Provides complete assessment information including:</p> <ul style="list-style-type: none"><li>• Name</li><li>• Risk Level (High, Medium, Low, Warning)</li><li>• Description</li><li>• Solution (includes location of patch)</li><li>• Related Web Links</li><li>• Relevant Advisories and Knowledge-Base Articles</li><li>• Link to Mitre web page containing Common Vulnerabilities and Exposures (CVE) information</li></ul>

Feature	Benefit																																																
<b>Safe Scanning</b>	Vulnerabilities are identified through engineered signatures, not simulated attacks. Computers will not be harmed and network bandwidth available to users will not be degraded due to a scan.																																																
<b>Accurate &amp; Complete</b>	<ul style="list-style-type: none"> <li>• Based on solid security research, solutions testing, and software product maintenance.</li> <li>• Scans for more Windows® vulnerabilities than other comparable tools.</li> <li>• Results in the least amount of “false positive” reports (reports that indicate a vulnerability where none exists).</li> <li>• Scans for third-party applications as well as operating system vulnerabilities.</li> <li>• Scans for vulnerabilities in Windows NT®, Windows® 95/98/2000/Me/XP, Windows® Server 2003, Red Hat™ &amp; Mandrake™ Linux®, Sun™ Solaris™ &amp; HP-UX UNIX®, Cisco® routers and HP printers.</li> <li>• A deep analysis is performed, not a surface validation.</li> </ul>																																																
<b>Customizable</b>	Provides a configuration editor to allow user tailoring of which vulnerabilities are scanned.																																																
<b>Updated Frequently During the Month</b>	New vulnerabilities are identified throughout the month and incorporated into an update available to customers on the STAT Premier website.																																																
<b>Reports</b>	<p>Extensive reporting capability that provides a full set of reports displaying information ranging from quick summary graphics to full and detailed disclosure of all vulnerabilities found.</p> <div data-bbox="602 1094 1328 1633" data-label="Figure"> <p><b>Vulnerability Summary Report (By Category)</b></p> <table border="1"> <thead> <tr> <th>Category</th> <th>Count</th> </tr> </thead> <tbody> <tr><td>Registry</td><td>22</td></tr> <tr><td>Denial of Service</td><td>21</td></tr> <tr><td>Web Browser</td><td>17</td></tr> <tr><td>Account Policy</td><td>13</td></tr> <tr><td>Password</td><td>10</td></tr> <tr><td>Unauthorized Access</td><td>8</td></tr> <tr><td>User Rights</td><td>7</td></tr> <tr><td>Log</td><td>6</td></tr> <tr><td>Privilege Elevation</td><td>5</td></tr> <tr><td>C2</td><td>4</td></tr> <tr><td>Info Gathering</td><td>3</td></tr> <tr><td>File Permission</td><td>2</td></tr> <tr><td>Backdoor</td><td>2</td></tr> <tr><td>Service</td><td>2</td></tr> <tr><td>Administrator</td><td>1</td></tr> <tr><td>Display</td><td>1</td></tr> <tr><td>Folder Permission</td><td>1</td></tr> <tr><td>Regedit</td><td>1</td></tr> <tr><td>Service Pack</td><td>1</td></tr> <tr><td>Share</td><td>1</td></tr> <tr><td>Source Routing</td><td>1</td></tr> <tr><td>Source Routing</td><td>1</td></tr> <tr><td>Unsafe Code</td><td>1</td></tr> </tbody> </table> </div> <p>Reports include:</p> <ul style="list-style-type: none"> <li>• Executive Summary</li> <li>• Network Summary</li> <li>• Vulnerability Summary</li> <li>• Detailed Vulnerability List</li> </ul>	Category	Count	Registry	22	Denial of Service	21	Web Browser	17	Account Policy	13	Password	10	Unauthorized Access	8	User Rights	7	Log	6	Privilege Elevation	5	C2	4	Info Gathering	3	File Permission	2	Backdoor	2	Service	2	Administrator	1	Display	1	Folder Permission	1	Regedit	1	Service Pack	1	Share	1	Source Routing	1	Source Routing	1	Unsafe Code	1
Category	Count																																																
Registry	22																																																
Denial of Service	21																																																
Web Browser	17																																																
Account Policy	13																																																
Password	10																																																
Unauthorized Access	8																																																
User Rights	7																																																
Log	6																																																
Privilege Elevation	5																																																
C2	4																																																
Info Gathering	3																																																
File Permission	2																																																
Backdoor	2																																																
Service	2																																																
Administrator	1																																																
Display	1																																																
Folder Permission	1																																																
Regedit	1																																																
Service Pack	1																																																
Share	1																																																
Source Routing	1																																																
Source Routing	1																																																
Unsafe Code	1																																																

Feature	Benefit
Industry Standard Compliant	Uses industry standard CVE identification scheme.
Integrated with Harris vision and framework	Integrates with STAT® Analyzer. Provides a bridge between policy creators and those responsible for policy enforcement.

## System Requirements

### Minimum and Recommended Hardware/Software/Administrative Requirements

- PC or compatible with Pentium® III or higher
- 256 MB RAM (512+ recommended, depending on number of targets scanned at one time)
- 40 MB free disk space
- 800 x 600 monitor resolution display (1024 x 768 recommended)
- CD ROM drive or an Internet connection
- Swap file size 1.5x to 2x larger than RAM for local host or small workgroup scans. 2x to 3x larger than RAM for network scans
- Windows NT® 4.0 SP 3 or higher / Windows® 2000 / XP
- User must have Administrative rights (See Minimum Administrative Requirements)
- TCP/IP, NetBEUI or Novell IPX/SPX protocols
- MDAC (Microsoft Data Access Component) 2.5 or later (For ODBC support. Default-loaded on Windows 2000/XP)
- Internet Explorer 4.0 or later - Used for Help and Web functions and some Dynamic Link Libraries (DLLs)

### Minimum Administrative Requirements

- For a full vulnerability analysis, the user must be logged into an account that is part of the Administrator's group.
- To perform analysis of other machines on the network, the user must be logged into the Domain with an account that is part of the Administrator's group.
- In order to analyze Windows NT, 2000, and XP workgroups, the user must be logged in as an administrative account that has access to every machine to be assessed.

## Summary

STAT Scanner is a security administration tool that helps keep network computer configurations up-to-date with current patches, security roll-ups, and service packs, resulting in a network that can best protect itself from intrusion. Network administrators can take advantage of years of security research and knowledge embedded in STAT Scanner to maintain their networks with minimal time and effort. STAT Scanner reduces the cost of maintaining network security by assessing the network and providing the administrator with the information to update the configuration or providing a single button solution that implements the selected corrective action. Updates for STAT Scanner are available every month via the STAT website [www.stat.harris.com](http://www.stat.harris.com).