



Precise Network-Based Threat Assessment

With more than 30,000 known software vulnerabilities¹ and countless configuration and access point threats, how can you possibly keep track of all of the potential threats to your network? The answer is PatchLink Scan™, a revolutionary advancement in network-based scanning from Lumension Security™. PatchLink Scan is a proven, Common Criteria EAL2 certified network-based scanner that will identify and display all assets and potential threats in your environment, quickly and with absolute precision.

- ▣ Complete identification and inventory of all devices on the network
- ▣ Accurate scans of all devices for software and configuration-based vulnerabilities
- ▣ Risk-based prioritization of identified threats
- ▣ Continuously updated vulnerability database for orderly remediation
- ▣ Comprehensive reports of scan results

Complete Asset Discovery and Inventory

The first step in securing your environment is understanding what devices and vulnerabilities are currently identified. You can only secure the devices you know about. PatchLink Scan thoroughly identifies and inventories all of the assets running on your network, including servers, desktops, laptops, routers, switches, printers, wireless access points, and more. This discovery can be performed using multiple inclusions and exclusions of IP ranges, Active Directory OU queries, Host names, Network Neighborhood enumerations, and imported lists. And discovery methods can be used separately or in conjunction, as PatchLink Scan transparently merges all results into a single, comprehensive asset list.

Severity	ID	Version	Source	Name	Category	ACERT	Advisory
High	W2892	80	STAT	Vector Markup Language Vulnerability	Unsafe Code		MS06-055
High	W2897	80	STAT	Windows Explorer WebViewFolderIcon Act...	Input Validation	2006-A-0...	MS06-057
High	W2899	80	STAT	XML Core Services 3.0 XSLT Handling Vul...	Arbitrary Code Ex...	2006-A-0...	MS06-061
High	W2919	80	STAT	XML Core Services 4.0 XSLT Handling Vul...	Arbitrary Code Ex...		MS06-061
High	W2920	80	STAT	XML Core Services 6.0 XSLT Handling Vul...	Arbitrary Code Ex...		MS06-061
High	W2942	80	STAT	XML 4.0 Core Services ActiveX Vulnerability	System Integrity	2006-A-0...	MS06-071
High	W2943	80	STAT	XML 6.0 Core Services ActiveX Vulnerability	System Integrity	2006-A-0...	MS06-071
High	W2950	80	STAT	IE 6 Cumulative Patch Missing (December...	Unsafe Code		MS06-072

PatchLink Scan - View of Network Targets

Rapid, Accurate Vulnerability Assessments

PatchLink Scan provides accurate vulnerability assessment using safe, adaptive network-based scanning techniques against a comprehensive vulnerability database. PatchLink Scan was designed to deliver a solid balance of scan speed and accuracy via its adaptive scan techniques and false response correlation technology. Through deep inspection of target systems that includes redundant file attribute and registry value correlation, as well as SSH tunneling and authenticated OS fingerprinting refinement, the scanner identifies all software threats, including missing patches, out-of-date antivirus signatures, worms, trojans, and more. The scan also runs detailed configuration checks on ports, users, shares, groups, agents and services. To guarantee thorough analysis, the solution is able to adapt its scanning technique based on its level of access, with the ability to run anonymous scans against target systems upon which it cannot authenticate.

Features & Benefits

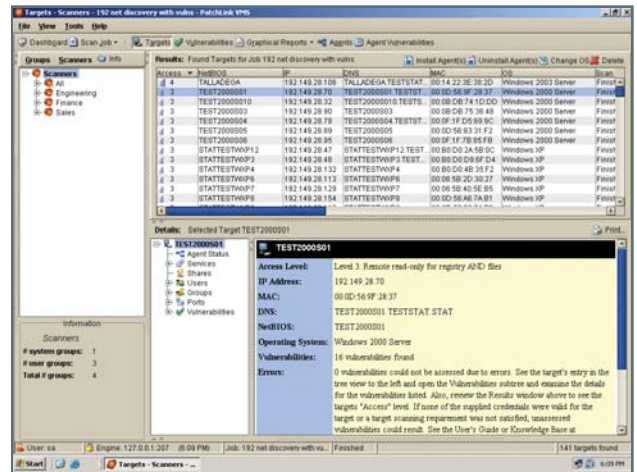
- ▣ **Adaptive Scanning** : Flexible scanning based on access-levels including credentialed and null-based scans
- ▣ **Auto Updating** : Schedule and automate recurring scan tasks to run on a daily, weekly or monthly basis
- ▣ **Complete Asset Discovery** : Identify all network devices and perform configuration checks on ports, services, users, shares and groups
- ▣ **Common Criteria EAL2 Certified** : Complies with the all specified security requirements of the CCS Certification Body
- ▣ **Comprehensive Coverage** : Over 4000 vulnerability audits with support across Windows, POSIX and infrastructure devices.
- ▣ **Comprehensive Reporting** : Ability to create and export numerous high-level or detailed reports of all scan data
- ▣ **Consolidated Views** : Multiple scans can be merged together to form a more comprehensive security posture
- ▣ **Highly Scalable** : Multiple instances of the scan engine can be deployed and controlled remotely or locally
- ▣ **Non-Disruptive Scanning** : Safe scans using standard networking protocols with minimum impact to your network
- ▣ **Remediation Recommendations** : Extensive vulnerability database with informational resources and remediation recommendations
- ▣ **Risk-Based Prioritization** : Prioritize systems according to asset value and vulnerability criticalities using straight-forward equations
- ▣ **Role-Based Administration** : Enables distributed management of scan activity by user roles

Vulnerability Prioritization

PatchLink Scan helps you prioritize vulnerabilities based on asset criticality and vulnerability score-carding to aid in the remediation process. The solution includes an exhaustive information database of more than 4,000 vulnerabilities – full of actionable information to help you assess your threat levels and implement corrective actions. This resource is based on the knowledge of a team of expert security engineers who continually research security advisories, knowledge base papers and professional security group articles.

Comprehensive Management & Audit Reporting

To provide insightful and concise views of the security posture of your network, PatchLink Scan includes a wide range of standard reports that provide high-level or detailed information on vulnerabilities found by category, risk level, individual machine, and more – making it easier than ever to demonstrate policy and regulatory compliance. The reporting capability provides simple point and click capability to quickly ascertain the enterprise security posture relative to common industry tracking mechanisms such as SANS Top 20.



PatchLink Scan - View of Network Targets

“Frequent and thorough vulnerability assessment is a best practice that every company should follow.”

THE YANKEE GROUP

Remediation Detail	Remediation Description (All vulnerabilities contain this level of detail)
Name	The common industry tracking name for the vulnerability
Description	A short description of the vulnerability and potential exploits
Version	PatchLink Scan release when the vulnerability check was added to our database
Type	The exploit technique (191 Types) .e.g. Buffer overrun, Man-in-the-middle
Category	The exploit grouping (71 categories) e.g. Denial of Service, Privilege Escalation
Severity	High, Medium, Low, Warning, Information
References	CVE, Bugtraq, CERT, SANS, FEDCIRC, CIAC, DOD, ACERT, NAVCIRT, MS, Q, AFCERT, HP Package, RedHat Advisory, Mandrake Advisory, Progeny Advisory, Fedora Advisory, SUSE Advisory, Sun Package
Reference Links	Links to multiple security pages regarding particular vulnerabilities
Solution	Our tested remediation instructions
Application(s)	The impacted executable files or DLLs
Specific Info	Lists the registry and file reference for the vulnerability

Table 1: Detailed Vulnerability Information with Tested and Proven Remediation Instructions

Assess Your Environment Today

By leveraging PatchLink Scan, you are able to identify and correct weaknesses before they are exploited - no longer relying solely on reactive, defensive security measures. For more information on a free 30 day evaluation of PatchLink Scan visit us on the web at www.lumension.com.

Sources:

1. Computer Emergency Response Team (CERT) center of internet security expertise



Lumension Security
 15880 N Greenway-Hayden, Suite 100
 Scottsdale, AZ 85260
 480.970.1025 | www.lumension.com



PatchLink® - A Lumension Brand.

©2007 Lumension Security. All rights reserved. Lumension Security, the Lumension Security logo, and the PatchLink and Sanctuary product names and logos are either registered trademarks or trademarks of Lumension Security. In addition, other companies' names and products mentioned in this document, if any, may be either registered trademarks or trademarks of their respective owners.