

Retina CS Add-On: Patch Management Module

INTEGRATED, AUTOMATED, AGENTLESS PATCH MANAGEMENT

Combined with Retina CS Management, eEye's Patch Management Module closes the loop on vulnerabilities with **seamless patching from a single console.**

Difficulties with patch management present serious security risks and as a result, resource drain to stay up to date on the latest fixes. eEye created the Patch Management Add-on Module to close the loop on vulnerabilities and provide seamless patching from a single console, improving the efficiency and effectiveness of patch processes. Your IT Security team can quickly fix weaknesses for Microsoft and third-party applications using instant or scheduled patching, and see the big picture with end-to-end reporting on the entire patch management cycle.

REDUCE THE BURDEN OF PATCH MANAGEMENT

In combination with the Retina CS Management Console, our Patch Management Add-on Module streamlines the entire process from discovery and assessment to patch deployment and verification.

PATCH BASED ON RISK PROFILES

Map discovered vulnerabilities to available patches and utilize the advanced targeting and categorization of assets to more appropriately prioritize patch activities. Deploy and manage patches on all machines across Microsoft and third-party applications, such as Adobe.

AUTOMATED PATCHING PROCESS

Not only can you automatically download missing security updates based on discovered vulnerabilities, but you can also automatically deploy the missing patches or service-packs throughout your network at the end of scheduled scans.

OUT-OF-THE-BOX REPORTING

Out-of-the-box reporting gives you options such as patch availability reports, targets requiring patch, patch deployment results, and more.

BENEFITS

UTILIZE A SINGLE INTEGRATED PATCHING SOLUTION for Microsoft and third-party applications including Adobe (Distiller, Elements, Reader, Flash, Shockwave), and Mozilla (Firefox), and more.

GAIN COMPLETE VISIBILITY into all asset risks through end-to-end reporting

REDUCE EFFORT AND EXPENSE via integrated, agent-less patching processes built on the Microsoft WSUS engine that many organizations already use

IMPROVE THE EFFICIENCY AND EFFECTIVENESS OF PATCH PROCESSES with vulnerability correlation and targeting patches based on risk profiles

AUTOMATICALLY DOWNLOAD AND DEPLOY missing security updates based on discovered vulnerabilities



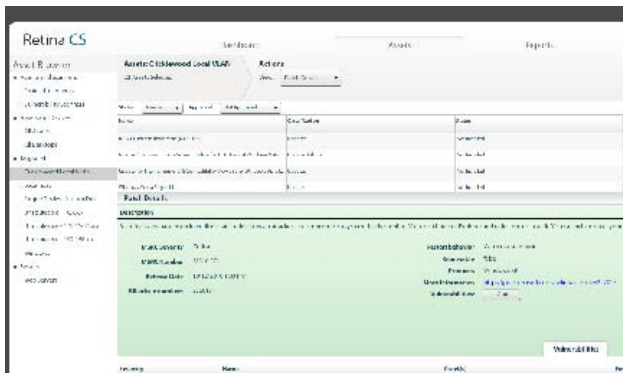
eEye Digital Security®

VULNERABILITY AND PATCH CORRELATION

Vulnerability and patch correlation allows you to link vulnerabilities to available patches, displayed via an easy-to-use dropdown list.

FULL CIRCLE VULNERABILITY MANAGEMENT

Cost effective, integrated, agent-less patch management provides full-circle vulnerability management from a single platform to save time and money.



Patch Management Asset Details Example

Patches

Title:	Windows Media Player 11
Description:	Windows Media Player 11 offers great new ways to store and enjoy digital media beyond music. It enables users to access all of your videos, pictures, and recorded TV on your computer. Play it, view it, organize it, sync it to a portable device for viewing on the go, or share with devices around your home—all from one place. After you install this item, you may have to restart your computer.
Classification:	Updates MSRC Severity: Unspecified
KB Articles:	929800
Title:	Update for Windows XP (KB932004)
Description:	The Remote Desktop Connection 7.0 client update enables you to use the new Remote Desktop Services features. These features are introduced in Windows 7 and in Windows Server 2008 R2 and are available for computers that are running Windows Vista Service Pack 1, Windows Vista Service Pack 2 or Windows XP Service Pack 3. After you install this item, you may have to restart your computer.
Classification:	Updates MSRC Severity: Unspecified
KB Articles:	932004

Required Patches Report Example

SYSTEM REQUIREMENTS

RETINA CS 2.0.X + AND RETINA INSIGHT 2.0.1 +

WINDOWS SERVER 2003 SP2 OR HIGHER (32-BIT), SERVER 2008 (32-BIT AND 64-BIT), OR SERVER 2008 R2 (64-BIT)

MICROSOFT SQL SERVER 2005 SP3 OR 2008 SP2 (STANDARD OR ENTERPRISE EDITIONS ONLY)

MICROSOFT SQL SERVER REPORTING SERVICES, ANALYSIS SERVICES, AND INTEGRATION SERVICES

INTEL DUAL CORE 2.0GHZ (OR COMPATIBLE, MINIMUM)

4GB MINIMUM / 8GB RECOMMENDED (REQUIRES X64 OS)

700MB SOFTWARE INSTALL / 40GB DATABASE MINIMUM / 30GB (PATCH REPOSITORY MINIMUM)

NETWORK INTERFACE CARD (NIC) WITH TCP/IP ENABLED

MICROSOFT .NET FRAMEWORK 3.5 (INCLUDED WITH INSTALLER)

MICROSOFT IIS 6.0 OR HIGHER ASP.NET

About eEye Digital Security

Since 1998, eEye Digital Security has made vulnerability management simpler and more effective by providing the only unified vulnerability and compliance management solution that integrates security risk discovery, prioritization, remediation, and reporting into a complete offering. Consistently the first to uncover critical vulnerabilities and prevent their exploit, eEye leverages its world-renowned research and development to strategically secure customer assets. Thousands of mid-to-large size organizations, including some of the most complex IT environments in the world, rely on eEye solutions to protect against the latest known, unknown, and zero-day vulnerabilities. [See more at www.eeye.com](http://www.eeye.com)

CONTACT INFORMATION

UNITED STATES
1.866.282.8276

NORTH AMERICA SALES
sales@eeye.com

GERMANY
+49 (0) 8031 2227 432

INTERNATIONAL SALES
sales.eu@eeye.com

UNITED KINGDOM
+44 (0) 20 8432 3490

www.eEye.com

111 THEORY, SUITE 250 | IRVINE, CALIFORNIA 92617