




# 3A03 – Security L cher schnell und effizient schlieen mit HP OpenView Radia

Alexander Meisel  
HP OpenView

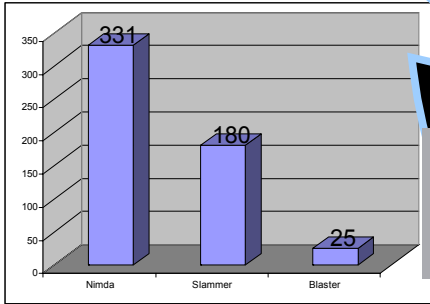


© 2004 Hewlett-Packard Development Company, L.P.  
The information contained herein is subject to change without notice




## Patch Management *Why do I need it?*

Time in days from issue of Bulletin to  
acknowledgement of exploit



Exploit	Time in days
Nimda	331
Slammer	180
Blaster	25



**Just in...**

- Bulletin MS04-011 issued April 13<sup>th</sup> 2004
- Sasser Exploit acknowledged 1<sup>st</sup> May 2004
- 18 days!



## Patch Management

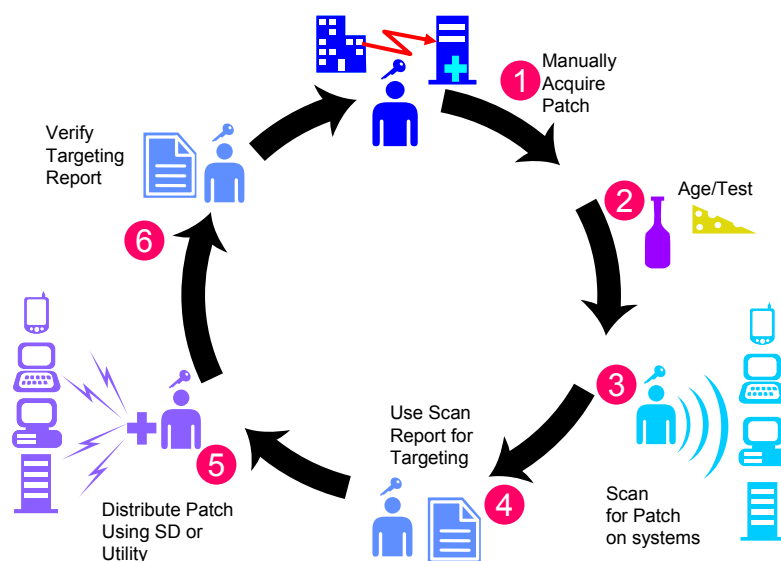
- Risikominimierung
  - Sicherheitslücken schaden dem Geschäft
    - *“The SQL Slammer worm caused between \$950 million and \$1.2 billion in lost productivity in it's first five days worldwide. (cnet news)”*
  - Anpassung an Veränderungen mit hoher Zuverlässigkeit wird benötigt
  - 95% der Lücken sind durch proaktives Patchmanagement vermeidbar\*
- Kosten
  - Implementation von automatisierten Patchmanagementlösungen reduzieren die Helpdesk-Calls und damit die Kosten
- Hohe Effektivität
  - IT muß 24/7 Service unterstützen und trotzdem hohe Skalierbarkeit, niedrige Kosten, Flexibilität erreichen

\* Source : CERT

3



## Patch Prozess





## Patch Process\*

1. **Audit machine** production environment to determine operational baseline (daily for servers, weekly for workstations)
2. **Confirm** that the **audit** has taken place and identify machines that have not been audited. (daily for servers, weekly for workstations)
3. **Check security web** sites to determine whether new patches are available. (Daily).
4. **Scan production environment** for required patches. (weekly).
5. **Assess patch prerequisites**, sequences and conflicts. (per required patch)
6. **Pilot patch release** in production environment. (per required patch)
7. **Deploy patch** release to production environment. (per patch)

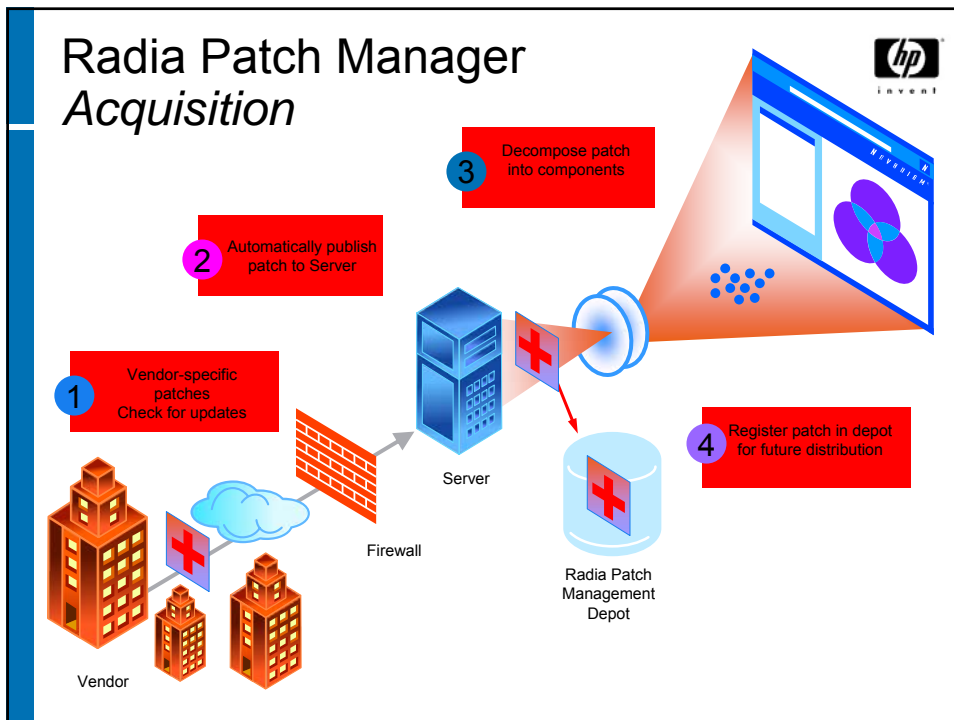
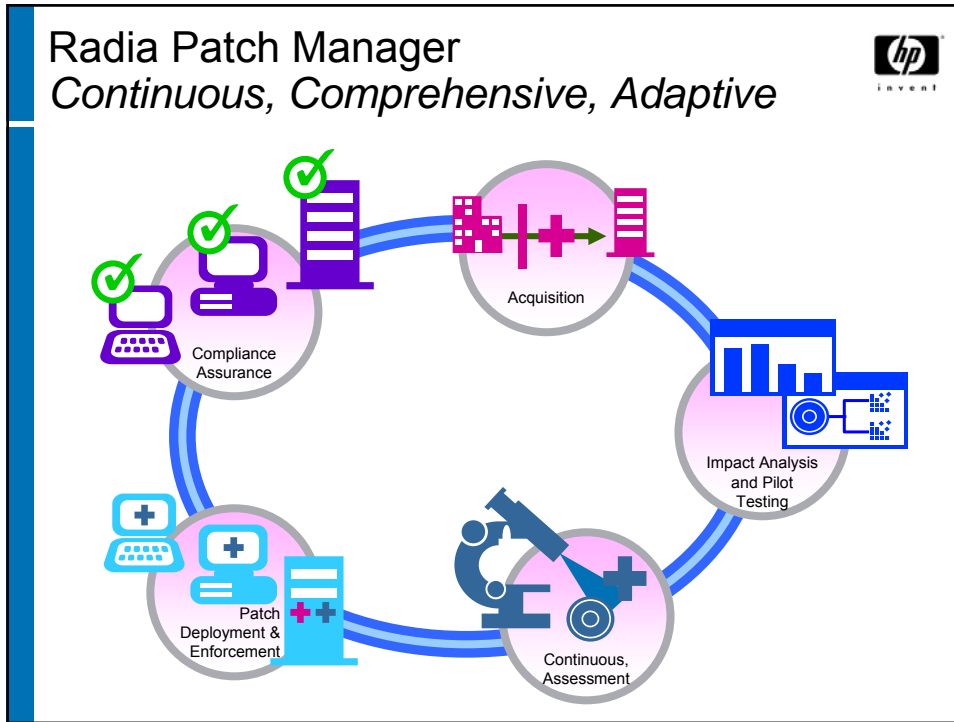


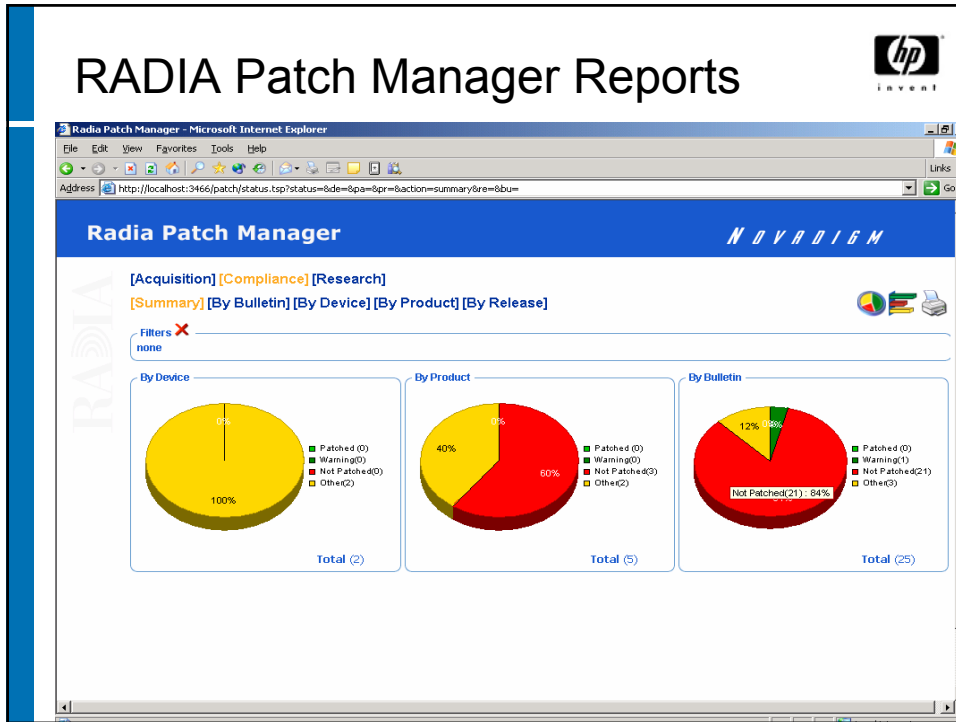
\*see Microsoft TechNet Patch Management Prozess



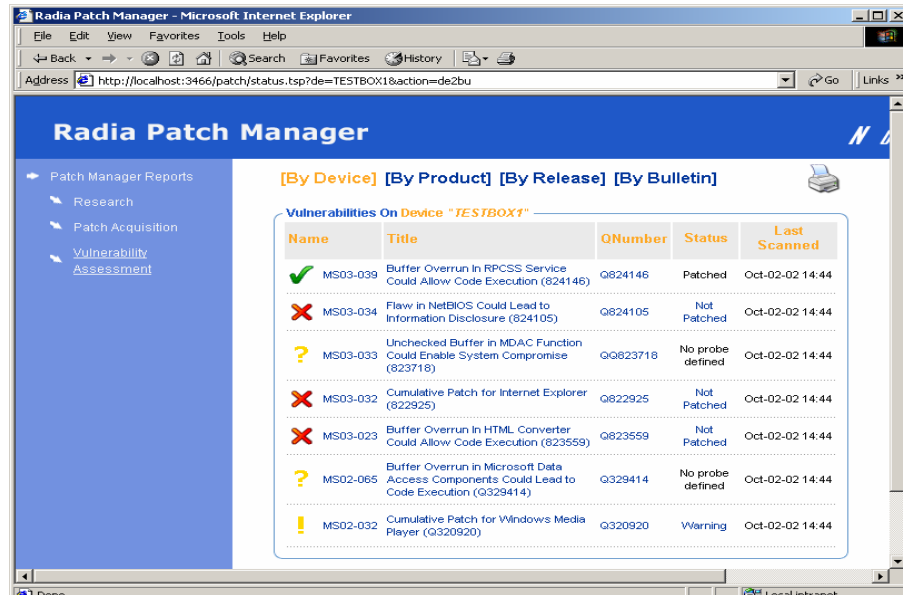
## Patch Management Prozess

- Viel Automatisierungspotential
- Lösungen für Client und Server Bereich notwendig
- Windows, Linux, UNIX ???





## RADIA Patch Manager Reports



**Radia Patch Manager** NOVADIGM

Patch Manager Reports  
 Research  
 Patch Acquisition  
 Vulnerability Assessment

[By Device] [By Product] [By Release] [By Bulletin]

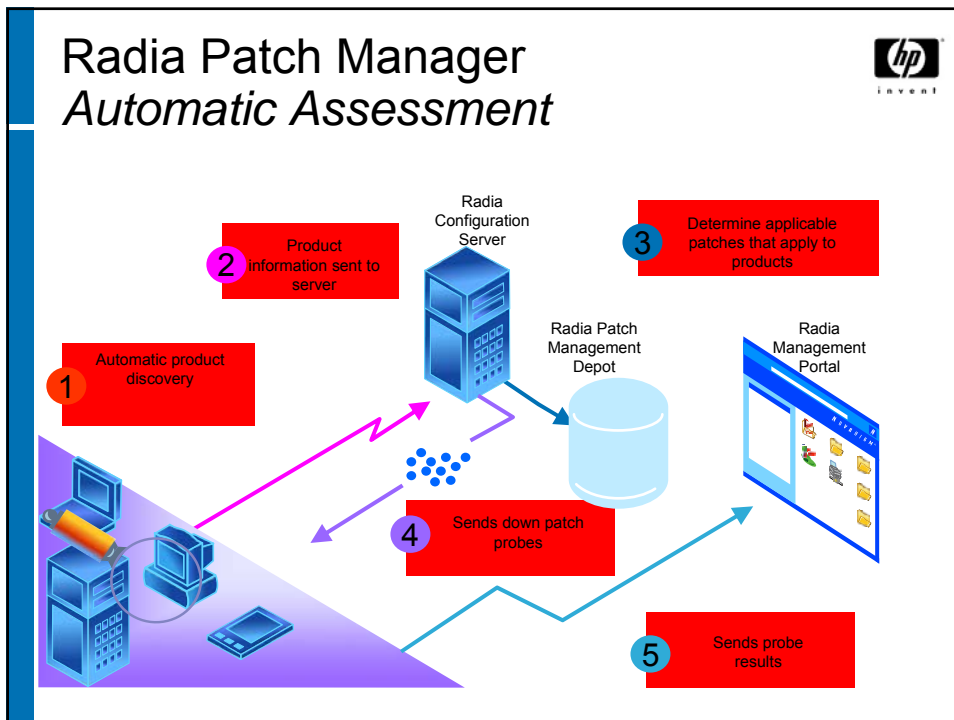
**Vulnerabilities On Device "TESTBOX1"**

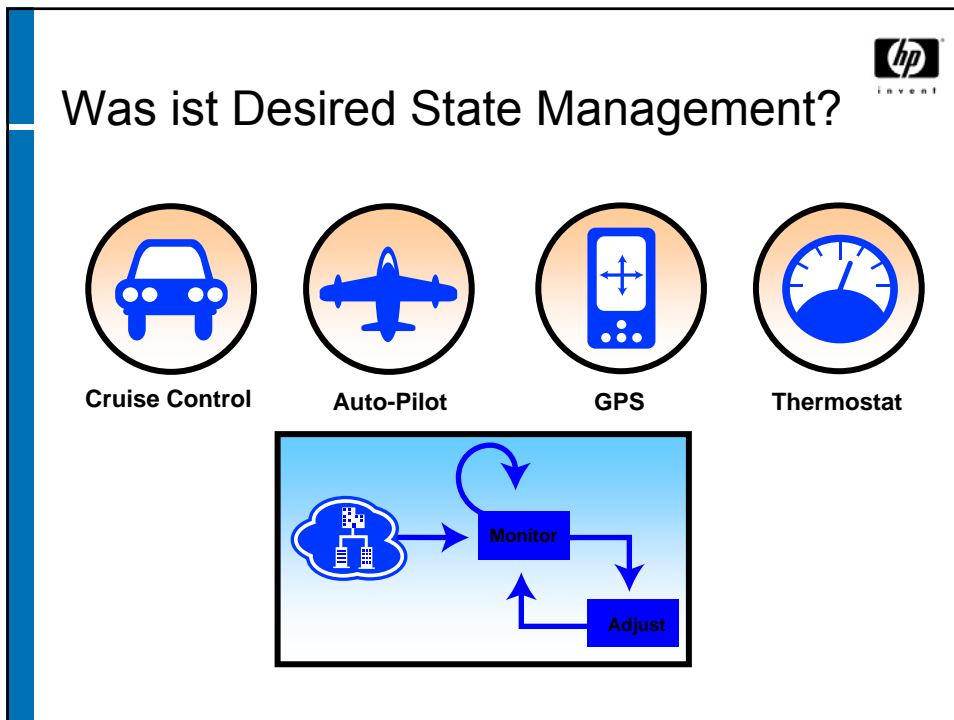
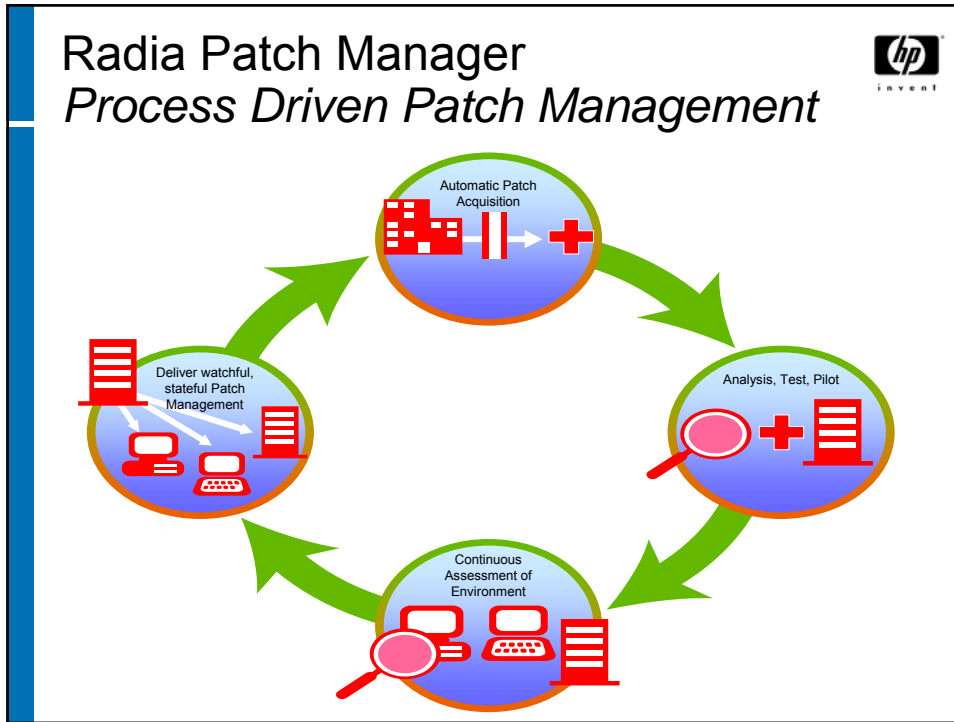
Name	Title	QNumber	Status	Last Scanned
✓ MS03-039	Buffer Overrun In RPCSS Service Could Allow Code Execution (824146)	Q824146	Patched	Oct-02-02 14:44
✗ MS03-034	Flaw in NetBIOS Could Lead to Information Disclosure (824105)	Q824105	Not Patched	Oct-02-02 14:44
? MS03-033	Unchecked Buffer in MDAC Function Could Enable System Compromise (823718)	Q823718	No probe defined	Oct-02-02 14:44
✗ MS03-032	Cumulative Patch for Internet Explorer (822925)	Q822925	Not Patched	Oct-02-02 14:44
✗ MS03-023	Buffer Overrun In HTML Converter Could Allow Code Execution (823559)	Q823559	Not Patched	Oct-02-02 14:44
? MS02-065	Buffer Overrun in Microsoft Data Access Components Could Lead to Code Execution (Q329414)	Q329414	No probe defined	Oct-02-02 14:44
! MS02-032	Cumulative Patch for Windows Media Player (Q320920)	Q320920	Warning	Oct-02-02 14:44

## Erweiterte Konflikt Analyse

The screenshot shows the Configuration Analysts interface. The main window lists various system modules. A dialog box titled 'Resource Conflict Detail - ACROPS2.DLL' is open, displaying the following information:

Property	After Install Analysis of Acrobat Reader 4.0	After Install Analysis of Acrobat Reader 4.0
File Path	C:\Program Files\Adobe\Acrobat 4.0\Reader	C:\Program Files\Adobe\Acrobat 4.0\Reader
File Name	AcroU32.dll	AcroU32.dll
File Size	150,136	150,136
File Version	0.0.0.0	0.0.0.0
File Attributes	Archive	Archive
File Type	Module	Module
Modification Date	AcroU32.dll	AcroU32.dll
Modification Time	0x01041F9	0x010409F
Modification Time	04.328#	04.328#
ImageBase	0x1000000	0x1000000
ImageSize	167,306	167,306
Package	PrivateBin, PrivateBuild	PrivateBin, PrivateBuild
Package	Base	Base
PackageType	DI	DI
PackageType	Unknown	Unknown







## Zusammenfassung

- Patch Management in heterogener Client und Server Umgebung (Windows, Linux, Solaris, HP-UX) schließt schnell Sicherheitslücken (\* later 2005)
- Automatische Akquise und Analyse der Verwundbarkeit
- Reduzierte Test-Aufwände durch Konflikt Analyse
- Desired State Management stellt dauerhaft sichere Umgebung sicher
- Objekt-orientiertes Modell ermöglicht Bandbreitensteuerung und einfachste Zuweisung auf Basis von Organisationsstrukturen (Verzeichnisse)