Are my systems ~~alive~~ secure?

IT SECURITY PATCH MONITORING WITH NAGIOS

Frank Migge, Manager Information Security Office

OPEN SOURCE MONITORING CONFERENCE on Nagios

Formerly known as "Nagios Konferenz"

Agenda

1. Vulnerabilities
   - Increasing Numbers
   - Enabling Factors
   - Focus on Operating Systems
   - Mitigation and Elimination Strategies
   - Vendor Response
   - The Challenges of Patching

2. Improving Patch Management
   - IT Infrastructure Vendor Review
   - Patch Monitoring for Windows
   - Patch Monitoring for AIX Unix
   - Patch Monitoring for Linux
   - Patch Monitoring for Cisco

3. Experience and Future

1. Vulnerabilities

Definition:

A weakness in system security procedures, system design, implementation, or internal controls that could be exploited impacting confidentiality, integrity or availability of the system.

Vulnerable systems become exploitable for a malicious person or automated malware (virus) using a variety of techniques like script code injection, SQL injection, buffer overflow, etc.

IT SECURITY PATCH MONITORING WITH NAGIOS

OPEN SOURCE MONITORING CONFERENCE on Nagios

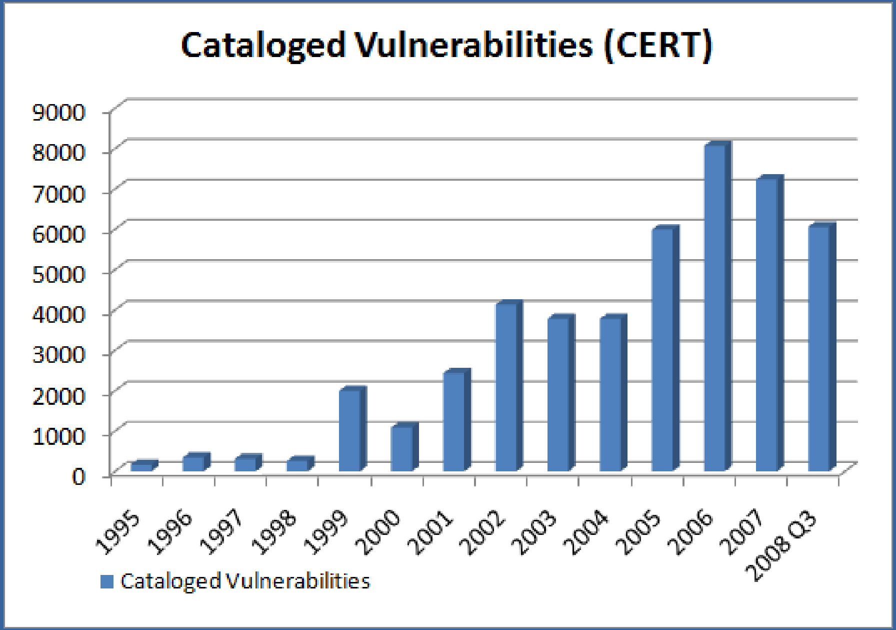
Formerly known as "Nagios Konferenz"

Vulnerabilities: Increasing Numbers

- Steep increase in recent vulnerabilities

Source: http://www.cert.org/stats/
CERT*, the **C**omputer **E**mergency **R**eadiness **T**eam, who coordinates communication during security emergencies and helps to prevent future incidents.

*CERT is one of the oldest institutions in IT Security, not to confuse with the US-CERT at http://www.us-cert.gov/



IT SECURITY PATCH MONITORING WITH NAGIOS

Reasons:

- increasing software complexity
- faster time-to-market (sell first – update later)
- Network connectivity built into everything
- Internet everywhere on the planet, greater pool of smart people on the “wrong” side

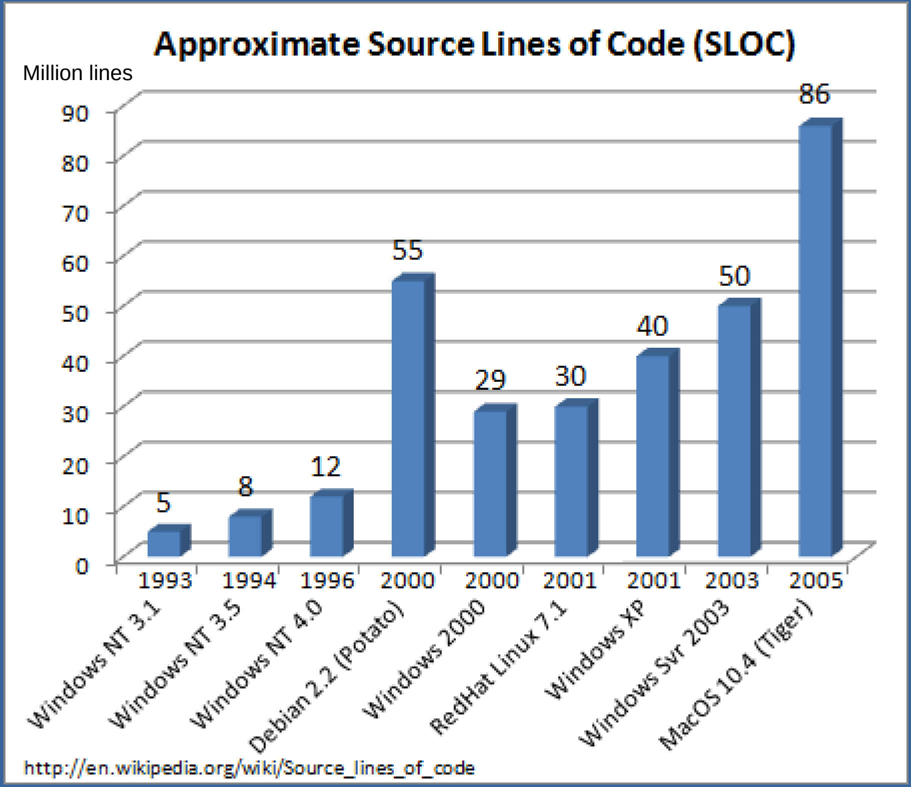
Focus on Operating Systems

- OS became the largest "piece" of SW:
  - Increased size due to progress in GUI design, device support, "features", connectivity, integrated applications
  - Increased required disk space

But also increased vulnerability.

"complexity is the worst enemy of security"

Bruce Schneier, http://www.schneier.com/crypto-gram-0003.html#8



http://en.wikipedia.org/wiki/Source_lines_of_code

IT SECURITY PATCH MONITORING WITH NAGIOS

- Network OS Vendor Cisco: Fighting with it's IOS complexity
  - 272722 different IOS Images known to the Cisco Feature Navigator (June 2009)
    Source: "Router Exploitation" - Felix 'FX' Lindner, BlackHat 2009, P19: The IOS Image Hell - http://www.blackhat.com/
  - CCO example: SOHO Router 1812 = 184 versions
  - Reasons: HW, IOS is still a single, large ELF binary
  - Which version is the latest? Which has bugs???

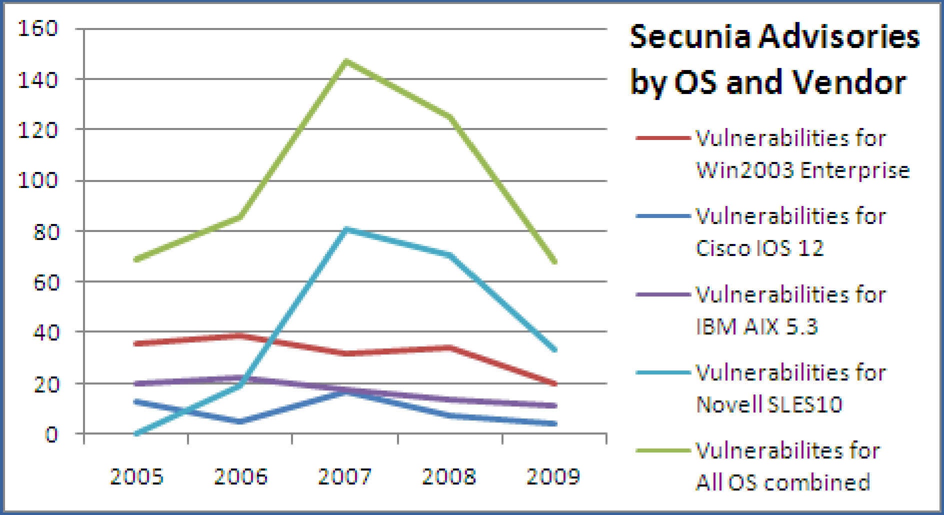
OPEN SOURCE MONITORING CONFERENCE on Nagios

Formerly known as "Nagios Konferenz"

Each Operating System vendor has a different vulnerability and risk “profile”

Common myth based on past experience: Windows has the highest risk.
As a target, yes, but not anymore by total numbers of vulnerabilities.

Why does Linux look so “bad”? Compared to a “barebone” OS, Linux distributions contain large numbers of applications in addition to the core OS



Source: http://secunia.com/advisories/vendor Secunia, established in 2002, is one of the leading vulnerability intelligence provider and distributors. It’s freely available Security Advisories list is used by IT Security teams.

Other risk criteria:

- Exposure, available exploits for vulnerabilities (virus)
- Available protection for OS (hardening, access control)
- Integration of additional HW and Devices
- Deployed applications
- Criticality for business

Vulnerability Mitigation and Elimination Strategies

OS Vendors: Secure Configuration Defaults

- disable insecure services
- enforce default password change

Secure Services

- using encryption and authentication

Implementation of Mitigation Features

- system firewalls or access control
- enhanced privilege separation and definitions

Patches, patches, patches …

IT SW Industry: Add-On Mitigation Software

Endpoint Security

- Virus Scanner (Client, Server and Storage side)
- Host-Based IDS
- Host-Based Firewall
- Device Control Wireless, USB

Configuration Control

- System scanner, Integrity Checker

The OS vendor patch response

New ways in patch provisioning, distribution, schedules and types:

- manual online patch download → built-in, automatic online patch service
  - Microsoft: Windows Update Service and Windows Update Website (ActiveX)
  - Linux: Novell Update Service (SLES), Redhat RHN Update Service
  - IBM: Service Update Management Assistant (SUMA)
- Simple vendor download site → distributed, policy-based patch-server architecture
  - Microsoft: WSUS
  - Novell: ZENworks Patch Management Server
  - IBM: Tivoli® Provisioning Manager

IT SECURITY PATCH MONITORING WITH NAGIOS

- New patch types: emergency (interim) patch, standard patch, service-pack
- ad-hoc patch releases → periodic patch days
  - Windows: monthly, first Tuesday in a month (Patch Tuesday, Black Tuesday)
  - Cisco: bi-annual, fourth Wednesday of March and September
  - IBM: quarterly schedule for service packs

Challenges of Patching - Why are systems unpatched?

- Patching costs resources (= money), real risk is difficult to quantify
- IT must balance operational costs vs. security risks
- IT operations cost is under high pressure (Outsourcing, SAS, HW consolidation)
- Patches need to be tested, any system change is a risk to current setup
- Too many vulnerabilities (while patching is scheduled, new patches are released)
- Vendors and security organizations announce ca 150 vulnerabilities/week
- Patch notification and distribution is not standardized

Vulnerability and Patch management is central part of IT Security Programs

IT SECURITY PATCH MONITORING WITH NAGIOS

IT Security teams constantly re-evaluate IT risk level based on new vulnerabilities, exploits, current system and application patch level, estimate window between identification of vulnerabilities and creation of exploits (shrinking). Among the common security tasks:

- Execution of periodic Vulnerability Scans
- Vulnerability Monitoring (time consuming, manual process)
- Escalation of perceived "high-risk" systems and situations

2. Improving IT Patch Management with Nagios

OS patch and version monitoring plug-in’s for Windows, AIX, Linux and Cisco

Frank Migge, Manager Information Security Office

- Plugin descriptions and links also available via http://www.monitoringexchange.org → “Articles”

2. Improving IT Patch Management

- Implementation of a vendor neutral patch status monitoring on all systems
- Implementation of immediate, standardized patch notification for all systems
- Leveraging existing systems inventory and monitoring escalation setup
- Real-time view into the current systems patch status and software versions

Patch status becomes just another indicator for "system health".

A task for Nagios®

IT SECURITY PATCH MONITORING WITH NAGIOS

Benefits:

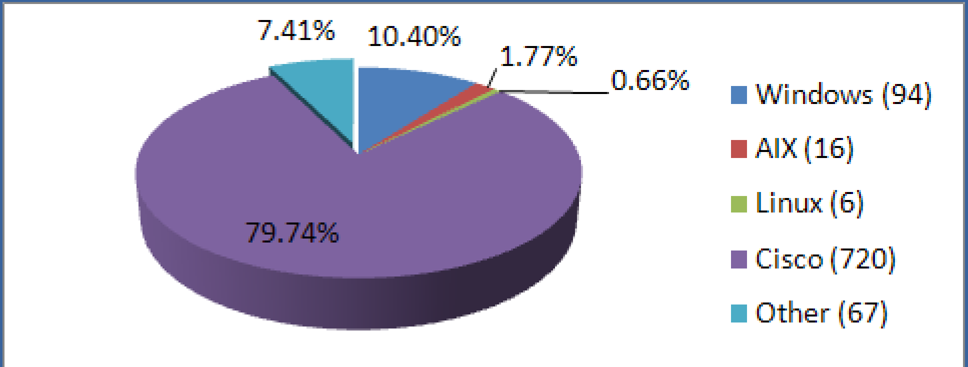
- Faster, direct and standardized notification to the support engineers
- Reduction of "human error" – missed systems / forgotten patches
- Fast identification of vulnerable systems
- Enforce and monitor patch policy compliance
- Highly visible patch accountability

Today's typical IT Infrastructure and Vendors:

Windows Servers	Traditional UNIX Servers	Linux Servers	Network Equipment	Appliances
• Office Backend • GroupWare • App Servers	• Database • Application • Web Servers	• Database • Application • Web Servers	• Switches • Routers • Firewalls	• Storage • VOIP • VMware hosts
Microsoft	***IBM, HP, SUN***	***RedHat, SuSE***	***Cisco***	***Others***

- Few network and server vendors, but each has it’s own distinctive patch management
- By implementing Nagios patch checks, we can cover almost all critical IT areas

IT SECURITY PATCH MONITORING WITH NAGIOS

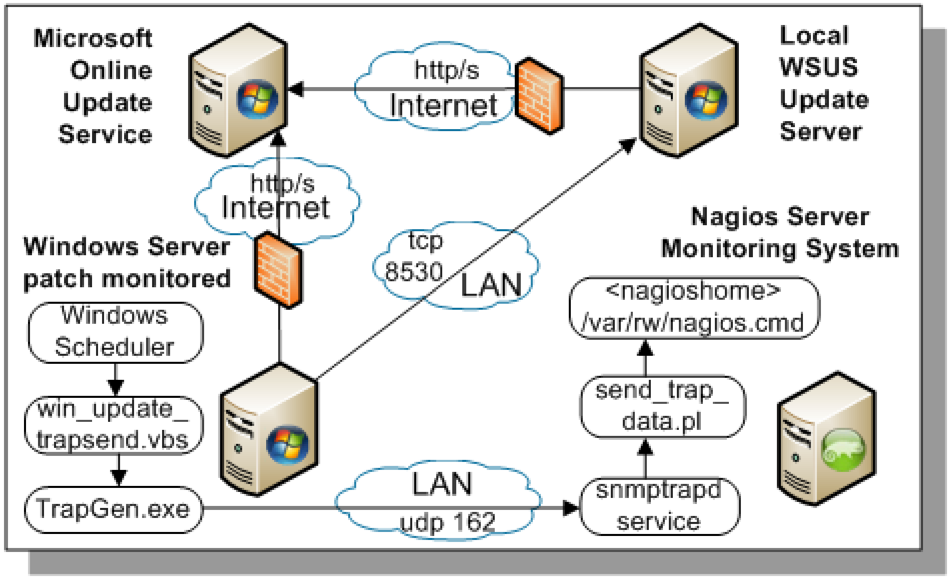


92.6% of all 903 PRD systems can be covered by patch monitoring

OS distribution in IT Infrastructure: We have a gap of 67 systems = 7.41%. Not covered systems are appliances, i.e. PBX and storage.

Nagios patch monitoring for Windows

prerequisites:	• Windows update service • SNMPtrapgen, [proxy]
data source	• Windows update service via Windows Scripting Host
plugin script	• win_update_trapsend.vbs (client) • send_trap_data.pl (Nagios server)
plugin execution	• passive, scheduled once a day • SNMP trap send to Nagios host



IT SECURITY PATCH MONITORING WITH NAGIOS

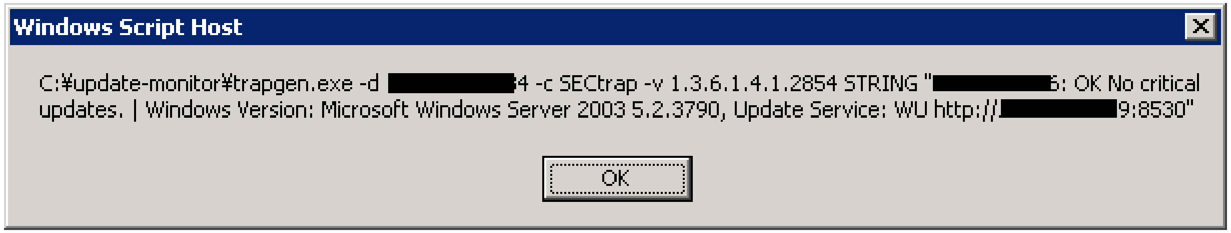
- Leverages Microsoft built-in scripting engine VBS for data collection
- requires extra binary for sending SNMPtraps to minimize ‘footprint’

  → no monitoring daemon installation
- Works well if update service is configured for Microsoft
- Less efficient with WSUS systems due to limited patch visibility

Patch monitoring: Microsoft Windows – Configure The Monitored System

1. Install, configure and test the programs trapgen.exe and win_update_trapsend.vbs

```
C:\update-monitor > cscript.exe -NoLogo C:\update-monitor\win_update_trapsend.vbs > C:\update-
monitor\ win_update_trapsend.log
```

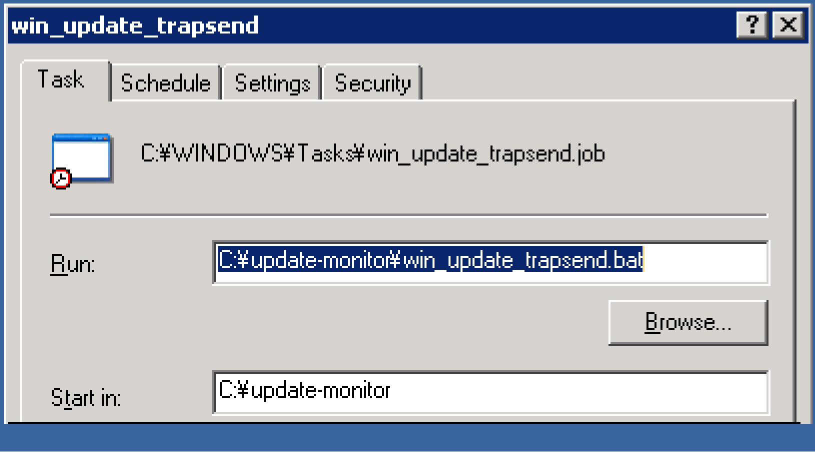


```
C:¥update-monitor¥trapgen.exe -d [redacted]4 -c SECtrap -v 1.3.6.1.4.1.2854 STRING "[redacted]6: OK No critical
updates. | Windows Version: Microsoft Windows Server 2003 5.2.3790, Update Service: WU http://[redacted]9:8530"
```

2. Create batch file and schedule daily execution job through Windows Scheduler

```
C:\update-monitor > edit win_update_trapsend.bat
cscript.exe -NoLogo C:\update-monitor\win_update_trapsend.vbs > C:\update-
monitor\win_update_trapsend.log
```

IT SECURITY PATCH MONITORING WITH NAGIOS



C:¥WINDOWS¥Tasks¥win_update_trapsend.job

Run: C:¥update-monitor¥win_update_trapsend.bat

Start in: C:¥update-monitor

The batch needs local administrative rights to execute.

Patch monitoring: Microsoft Windows – Nagios Setup

1. Configure the SNMPtrap service and install/update the traphandler ‘send_trap_data.pl’

```
nagios ~ # cat /etc/snmp/snmptrapd.conf
###############################################################################
# snmptrapd.conf:
# configuration file for configuring the ucd-snmp snmptrapd agent.
###############################################################################
# first, we define the access control
authCommunity log,execute,net SECtrap
# Win update traphandler: SNMPv2-MIB::snmpTrapOID.0 = RFC1155-SMI::enterprises.2854.0.1
traphandle RFC1155-SMI::enterprises.2854.0.1 /srv/app/nagios/libexec/send_trap_data.pl
```

2. Verify passive data submission into Nagios through the named pipe nagios.cfg

```
# grep EXTERNAL /srv/app/nagios/var/nagios.log
[1251126027] EXTERNAL COMMAND: PROCESS_SERVICE_CHECK_RESULT;[redacted];check_trap_winpatch;0;No
critical updates. | Windows Version: Microsoft Windows Server 2003 5.2.3790, Update Service: WU
http://[redacted]:8530
```

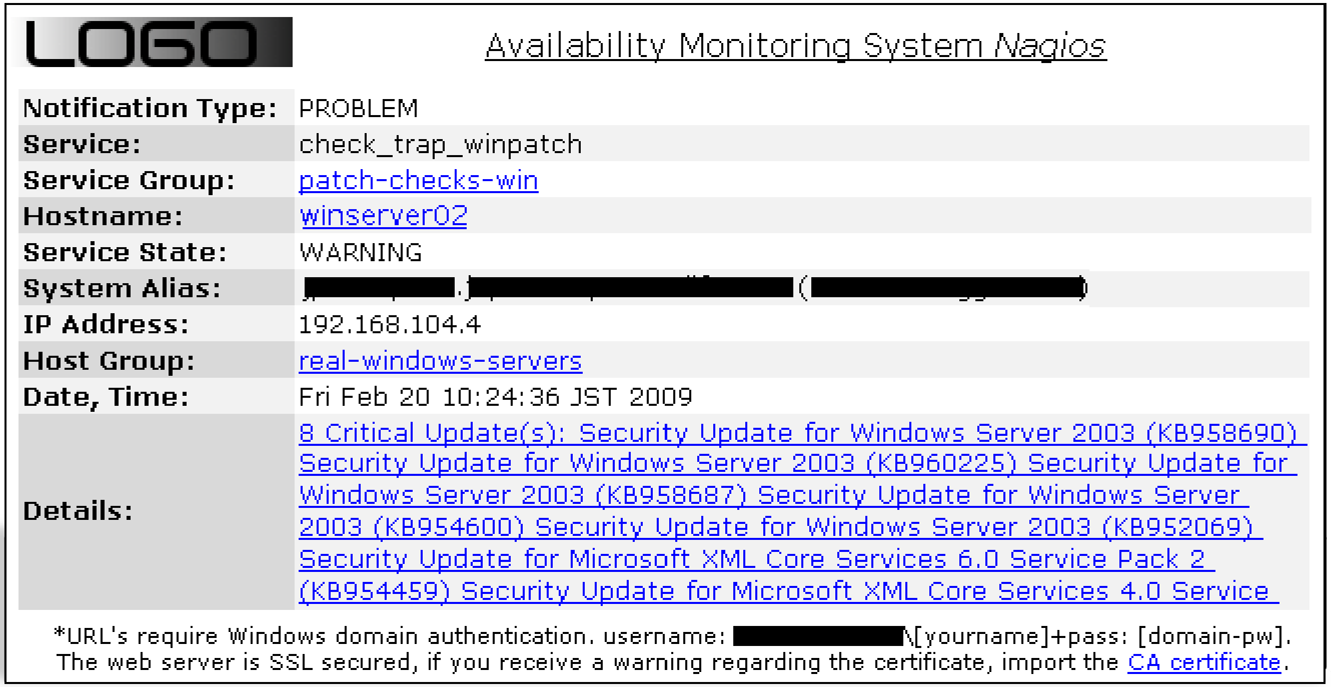
```
nagios ~ # vi /srv/app/nagios/etc/objects/patch-services-windows.cfg
###############################################################################
# Receive SNMP traps for Windows update status
###############################################################################
define service {
  use generic-patch-win
  hostgroup 2-windows-servers
  name check_trap_winpatch
  service_description check_trap_winpatch
  service_groups patch-checks-win, patch-compliance
}
```

3. Configure the new patch monitoring service

Using external commands in Nagios http://linux.com/archive/feature/153285

Patch monitoring: Microsoft Windows – Nagios Views

Service View and
E-Mail Notification

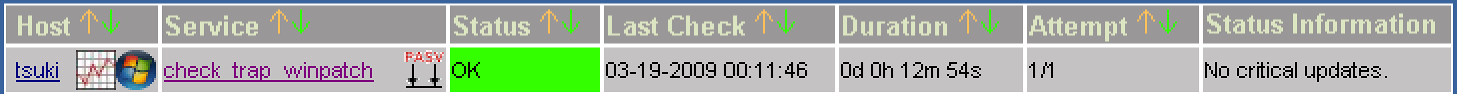


Availability Monitoring System *Nagios*

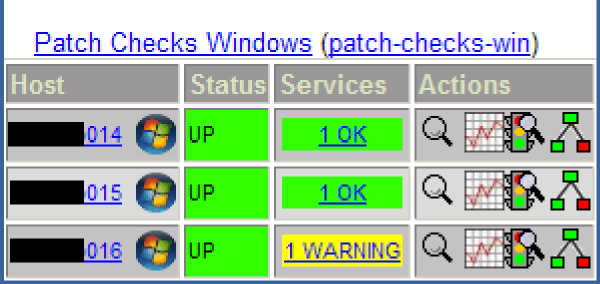
Notification Type:	PROBLEM
Service:	check_trap_winpatch
Service Group:	patch-checks-win
Hostname:	winserver02
Service State:	WARNING
System Alias:	[redacted].[redacted]([redacted])
IP Address:	192.168.104.4
Host Group:	real-windows-servers
Date, Time:	Fri Feb 20 10:24:36 JST 2009
Details:	8 Critical Update(s): Security Update for Windows Server 2003 (KB958690) Security Update for Windows Server 2003 (KB960225) Security Update for Windows Server 2003 (KB958687) Security Update for Windows Server 2003 (KB954600) Security Update for Windows Server 2003 (KB952069) Security Update for Microsoft XML Core Services 6.0 Service Pack 2 (KB954459) Security Update for Microsoft XML Core Services 4.0 Service

*URL's require Windows domain authentication. username: [redacted]\[yourname]+pass: [domain-pw].
The web server is SSL secured, if you receive a warning regarding the certificate, import the CA certificate.

IT SECURITY PATCH MONITORING WITH NAGIOS

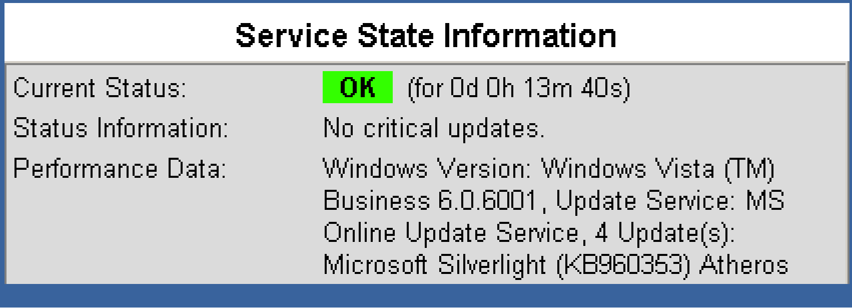


Host ↑↓	Service ↑↓	Status ↑↓	Last Check ↑↓	Duration ↑↓	Attempt ↑↓	Status Information
tsuki	check_trap_winpatch	OK	03-19-2009 00:11:46	0d 0h 12m 54s	1/1	No critical updates.



Patch Checks Windows (patch-checks-win)

Host	Status	Services	Actions
[redacted]014	UP	1 OK	
[redacted]015	UP	1 OK	
[redacted]016	UP	1 WARNING	

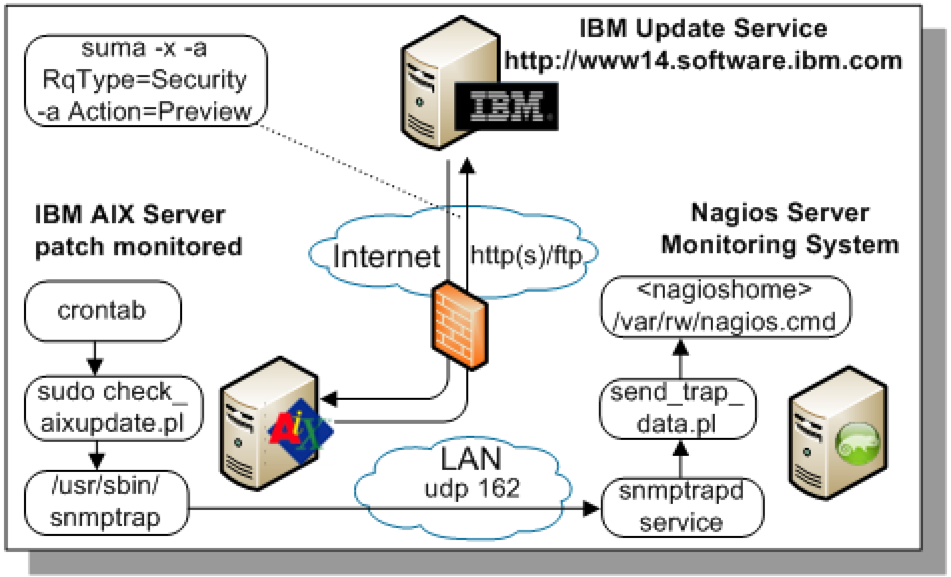


Service State Information

Current Status:	OK (for 0d 0h 13m 40s)
Status Information:	No critical updates.
Performance Data:	Windows Version: Windows Vista (TM) Business 6.0.6001, Update Service: MS Online Update Service, 4 Update(s): Microsoft Silverlight (KB960353) Atheros

Nagios patch monitoring for IBM AIX 5.3

prerequisites:	• IBM update service • SSH Service, [proxy]
data source	• SUMA
plugin script	• check-rug-update.pl (client) • check_snmp_extend.sh (svr)
plugin execution	• active, scheduled once a day • Passive, scheduled once a day



```
suma -x -a RqType=Security -a Action=Preview
```

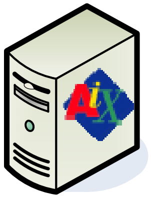
IT SECURITY PATCH MONITORING WITH NAGIOS

- The most 'conservatively' patched systems
- Least experienced staff needs the most help
- AIX is more secure in terms of less SW vulnerabilities
- AIX is weak in configuration due to the OS being quite 'old'

Patch monitoring: IBM AIX 5.3 – Configuring the Monitored System

1. Configure and verify the “Service Update Management Assistant" SUMA

```
$ sudo suma -c -a HTTP_PROXY=http://192.168.100.184:80/
$ sudo suma -c -a DL_TIMEOUT_SEC=10
$ sudo suma -c |grep HTTP_PROXY
 HTTP_PROXY=http://192.168.100.184:80/
$ sudo suma -c
…
```



SLES10

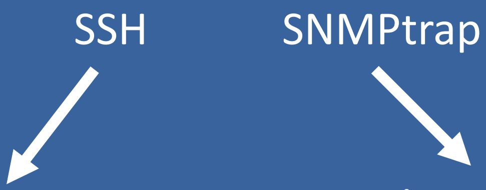
2. Install the plugin script ‘check-aix-update.pl’ or ‘aix_update_trapsend.pl’

```
$ sudo /scripts/check-aix-update.pl
WARNING - 211 update(s) available: X11.Dt.lib Version 5.3.7.2 X11.Dt.rte Version 5.3.7.3
X11.apps.rte Version 5.3.7.1 X11.base.lib Version 5.3.7.2 X11.base.rte Version 5.3.7.5
bos.64bit Version 5.3.7.7 bos.acct Version 5.3.7.8 bos.adt.base Version 5.3.7.3 bos.adt.debug
Version 5.3.7.3 bos.adt.include Version 5.3.7.7 bos.adt.insttools Version 5.3.7.2

... perfagent.tools Version 5.3.7.4 printers.rte Version 5.3.7.2|OS Version 5300-07-01-0748,
Proxy http://10.253.100.184:80/, Update-URL www14.software.ibm.com/webapp/set2/fixget
```

IT SECURITY PATCH MONITORING WITH NAGIOS

3. Decide the how to call and return the check result:



SSH

SNMPtrap

check-aix-update.pl

ssh user@aixhost "sudo /scripts/check-aix-update.pl"

aix_update_trapsend.pl

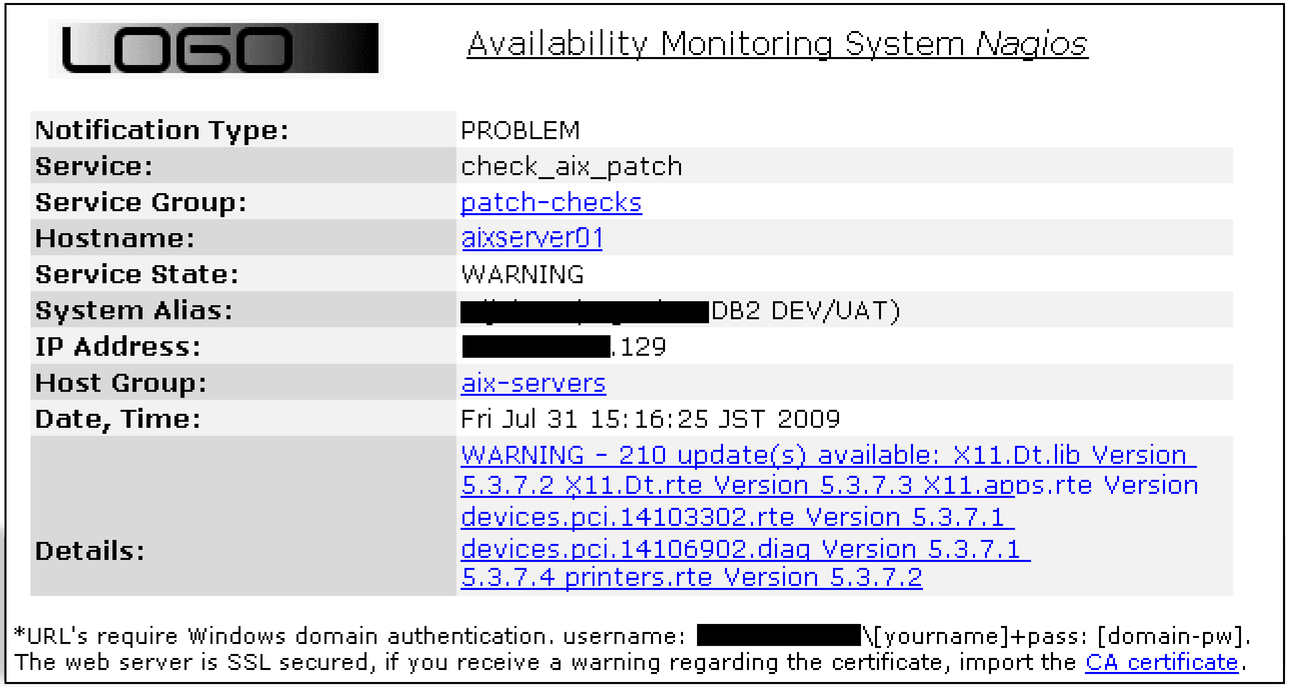
cron-scheduled once a day

Patch monitoring: IBM AIX 5.3 – Nagios Views

OPEN SOURCE MONITORING CONFERENCE on Nagios

Formerly known as "Nagios Konferenz"

Service Views and
E-Mail Notification

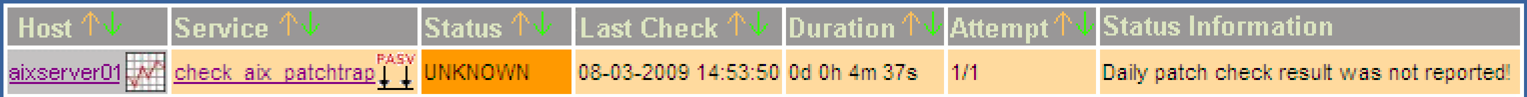


Availability Monitoring System *Nagios*

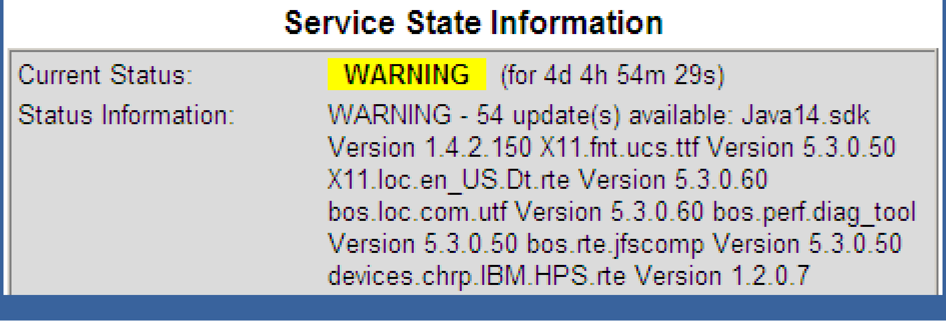
Notification Type:	PROBLEM
Service:	check_aix_patch
Service Group:	patch-checks
Hostname:	aixserver01
Service State:	WARNING
System Alias:	[redacted]DB2 DEV/UAT)
IP Address:	[redacted].129
Host Group:	aix-servers
Date, Time:	Fri Jul 31 15:16:25 JST 2009
Details:	WARNING - 210 update(s) available: X11.Dt.lib Version 5.3.7.2 X11.Dt.rte Version 5.3.7.3 X11.apps.rte Version devices.pci.14103302.rte Version 5.3.7.1 devices.pci.14106902.diag Version 5.3.7.1 5.3.7.4 printers.rte Version 5.3.7.2

*URL's require Windows domain authentication. username: [redacted]\[yourname]+pass: [domain-pw]. The web server is SSL secured, if you receive a warning regarding the certificate, import the CA certificate.

IT SECURITY PATCH MONITORING WITH NAGIOS

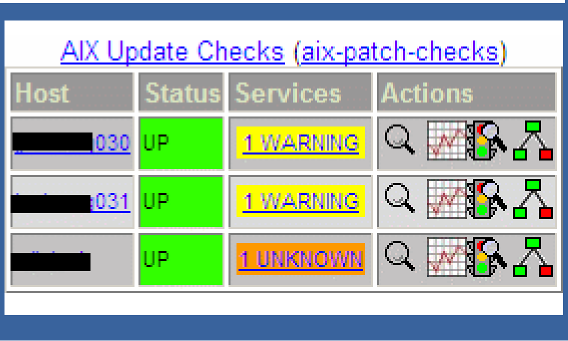


Host	Service	Status	Last Check	Duration	Attempt	Status Information
aixserver01	check_aix_patchtrap PASV	UNKNOWN	08-03-2009 14:53:50	0d 0h 4m 37s	1/1	Daily patch check result was not reported!



Service State Information

Current Status:	WARNING (for 4d 4h 54m 29s)
Status Information:	WARNING - 54 update(s) available: Java14.sdk Version 1.4.2.150 X11.fnt.ucs.ttf Version 5.3.0.50 X11.loc.en_US.Dt.rte Version 5.3.0.60 bos.loc.com.utf Version 5.3.0.60 bos.perf.diag_tool Version 5.3.0.50 bos.rte.jfscomp Version 5.3.0.50 devices.chrp.IBM.HPS.rte Version 1.2.0.7

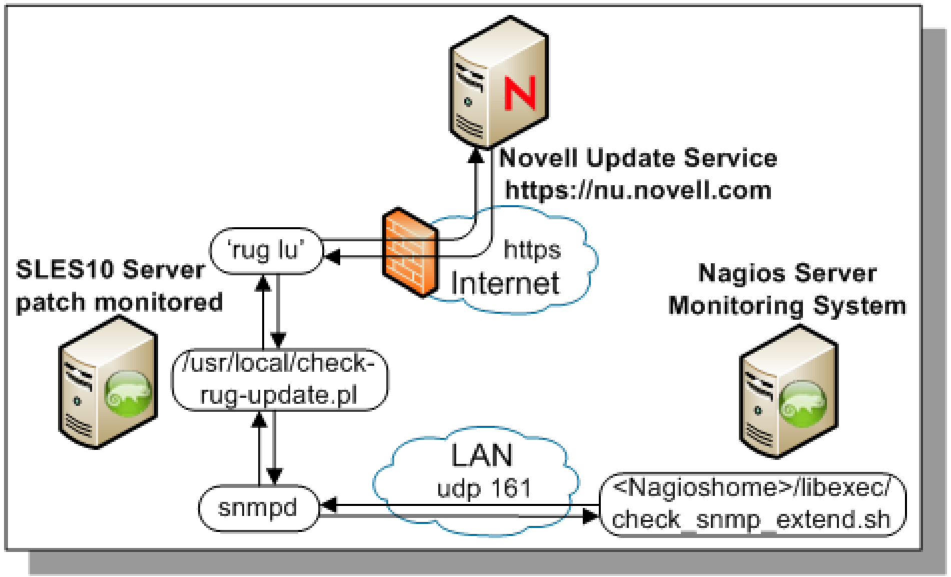


AIX Update Checks (aix-patch-checks)

Host	Status	Services	Actions
[redacted]030	UP	1 WARNING	
[redacted]031	UP	1 WARNING	
[redacted]	UP	1 UNKNOWN	

Patch monitoring: Novell Linux SLES10 - Overview

prerequisites:	• Novell update service • SNMP service, [proxy]
data source	• ZENworks zmd service via rug
plugin script	• check-rug-update.pl (client) • check_snmp_extend.sh (svr)
plugin execution	• active, scheduled once a day • SNMP request to SNMP extend



- Depends on 'rug' and novell-zmd service

  → zmd service 'zombies' experienced due to commit issues in sqlite backend

- Due to high frequency of Linux patch releases (weekly), big benefit

Patch monitoring: Novell Linux SLES10 – Configuring the Monitored System

1. Configure and verify the SLES Zenworks update service, using the 'rug' command

```
# rug lu
 S | Catalog             | Bundle | Name       | Version    | Arch
 --+---------------------+--------+-----------+-----------+-------
   | SLES10-SP2-Online |        | Spident   | 0.9-74.24 | noarch

# ./check-rug-update.pl
WARNING - 1 update(s) available: SPident Version 0.9-74.24
```

2. Install and test the plugin script ‘check-rug-update.pl’

```
# ./check-rug-update.pl --run-rug
OK - system is up to date

# cat ./test
 S | Catalog             | Bundle | Name       | Version    | Arch
 --+---------------------+--------+-----------+-----------+-------
   | SLES10-SP2-Online |        | Spident   | 0.9-74.24 | noarch

# ./check-rug-update.pl --file=test WARNING - 1 update(s) available: SPident Version 0.9-74.24
```

IT SECURITY PATCH MONITORING WITH NAGIOS

3. Configure and test the remote plugin access through the UCD Net-SNMP service

```
# echo "extend nagiosupdate /srv/app/nagios/libexec/check-rug-update.pl
--run-rug“ >> /etc/snmp/snmpd.conf

# /etc/init.d/snmpd restart
Shutting down snmpd: done
Starting snmpd

# snmpget -v 2c -c myread 127.0.0.1 NET-SNMP-EXTEND-MIB::nsExtendOutputFull.
“nagiosupdate"

NET-SNMP-EXTEND-MIB::nsExtendOutputFull.“nagiosupdate" = STRING: No updates
are available.
```

Patch monitoring: Novell Linux SLES10 – Nagios Setup

1. Get, install and test the ‘check_snmp_extend.sh’ script as a plugin

```
/srv/app/nagios/libexec # cp /tmp/check_snmp_extend.sh .

/srv/app/nagios/libexec # ls -l check_snmp_extend.sh
-rwxr-x--- 1 nagios nagios 1979 2008-10-02 16:50 check_snmp_extend.sh

/srv/app/nagios/libexec # ./check_snmp_extend.sh Syntax: check_snmp_extend.sh ipaddr community
/srv/app/nagios/libexec # ./check_snmp_extend.sh 192.168.11.22 myread nagiosupdate
OK - system is up to date
```

2. Configure the new plugin in the Nagios command.cfg section

```
/srv/app/nagios/etc/objects # vi commands.cfg

# 'check_snmp_extend' command definition
# syntax: check_snmp_extend.sh host-ip snmp-community extend-name
define command{
  command_name check_snmp_extend
  command_line $USER1$/check_snmp_extend.sh $HOSTADDRESS$ $ARG1$ $ARG2$
}
```

Nagios

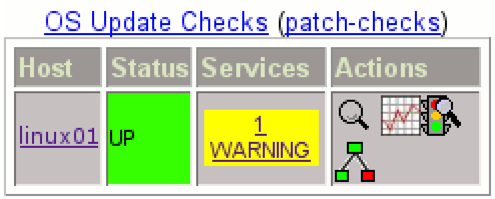
```
/srv/app/nagios/etc/objects # vi sles10-patch-services.cfg

###############################################################################
# SLES10 OS Patch Update Check via SNMP extend scripts
###############################################################################
define service {
  use generic-patch
  host_name ml08460
  name check_snmp_extend
  service_description check_patch_sles10
  check_command check_snmp_extend!myread!nagiosupdate
}
```

3. Configure the new patch monitoring service

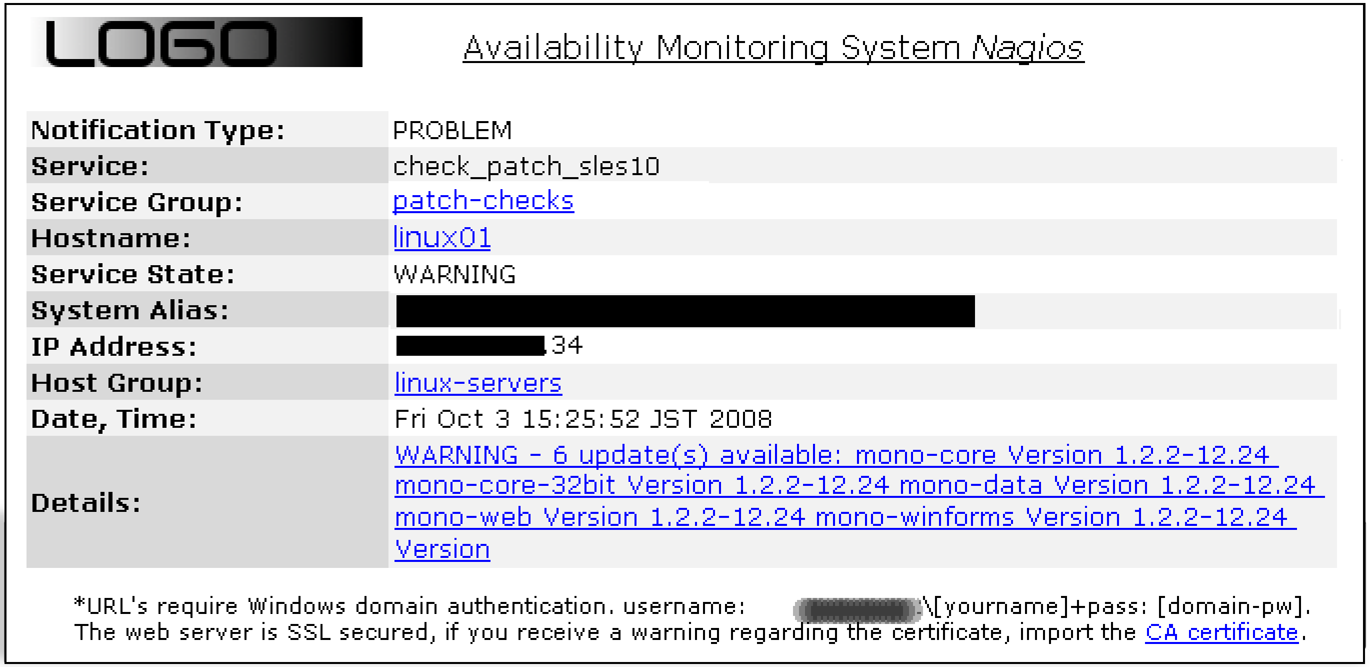
Patch monitoring: Novell Linux SLES10 – Nagios Views

Service View and
E-Mail Notification
(HTML formatted e-mail body
with embedded service links,
send through /usr/bin/mutt)



OS Update Checks (patch-checks)

Host	Status	Services	Actions
linux01	UP	1 WARNING	

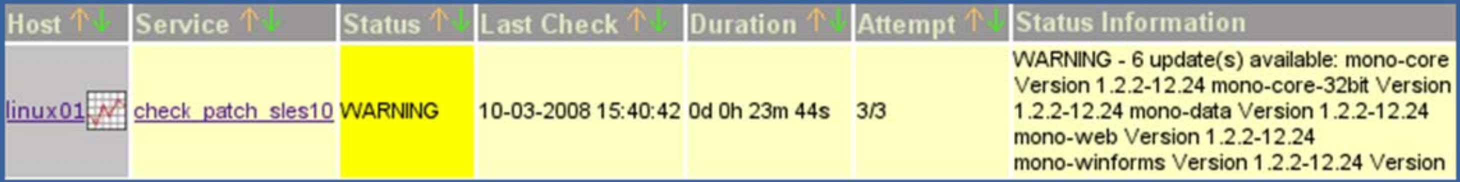


LOGO Availability Monitoring System *Nagios*

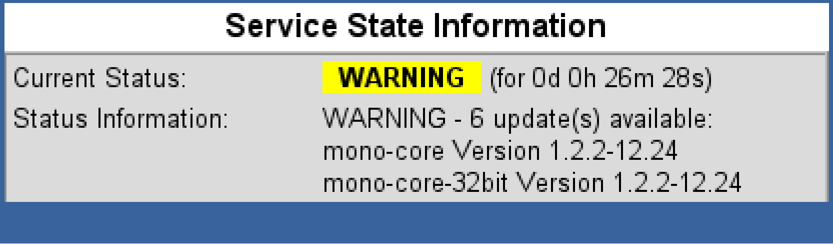
Notification Type:	PROBLEM
Service:	check_patch_sles10
Service Group:	patch-checks
Hostname:	linux01
Service State:	WARNING
System Alias:	[redacted]
IP Address:	[redacted]34
Host Group:	linux-servers
Date, Time:	Fri Oct 3 15:25:52 JST 2008
Details:	WARNING - 6 update(s) available: mono-core Version 1.2.2-12.24 mono-core-32bit Version 1.2.2-12.24 mono-data Version 1.2.2-12.24 mono-web Version 1.2.2-12.24 mono-winforms Version 1.2.2-12.24 Version

*URL's require Windows domain authentication. username: [redacted]\[yourname]+pass: [domain-pw].
The web server is SSL secured, if you receive a warning regarding the certificate, import the CA certificate.

IT SECURITY PATCH MONITORING WITH NAGIOS



Host ↑↓	Service ↑↓	Status ↑↓	Last Check ↑↓	Duration ↑↓	Attempt ↑↓	Status Information
linux01	check_patch_sles10	WARNING	10-03-2008 15:40:42	0d 0h 23m 44s	3/3	WARNING - 6 update(s) available: mono-core Version 1.2.2-12.24 mono-core-32bit Version 1.2.2-12.24 mono-data Version 1.2.2-12.24 mono-web Version 1.2.2-12.24 mono-winforms Version 1.2.2-12.24 Version

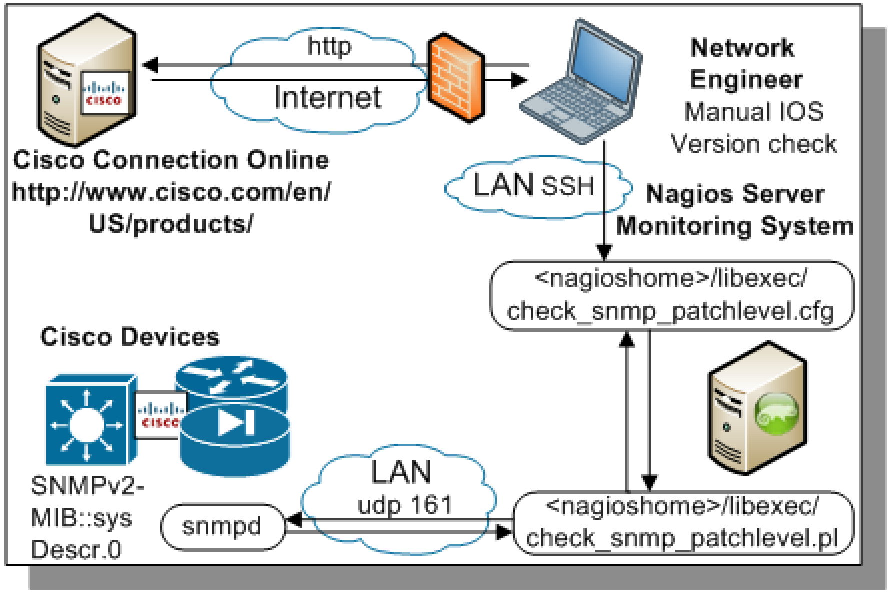


Service State Information

Current Status:	**WARNING** (for 0d 0h 26m 28s)
Status Information:	WARNING - 6 update(s) available: mono-core Version 1.2.2-12.24 mono-core-32bit Version 1.2.2-12.24

Nagios patch monitoring for Cisco IOS, ASA, PIX

prerequisites:	• SNMP service access • Cisco CCO account
data source	• SNMPv2 MIB "sysDescr"
plugin script	• check_snmp_patchlevel.pl • check_snmp_patchlevel.cfg
plugin execution	• active, scheduled once a day • SNMP request to SNMP MIB


http
Internet
Network Engineer
Manual IOS Version check
Cisco Connection Online
http://www.cisco.com/en/US/products/
LAN SSH
Nagios Server Monitoring System
<nagioshome>/libexec/check_snmp_patchlevel.cfg
Cisco Devices
SNMPv2-MIB::sysDescr.0
snmpd
LAN
udp 161
<nagioshome>/libexec/check_snmp_patchlevel.pl

IT SECURITY PATCH MONITORING WITH NAGIOS

- Cisco is ‘conservatively’ patched due to risk and effort (reboot, cumbersome rollback)
- Big benefit for standardizing OS versions and identifying ‘rogue’ devices
- Network device numbers greatly surpass server numbers

Patch monitoring: Cisco IOS, ASA, PIX – Cisco Setup

1. Cisco SNMP service configuration eample

```
Router # conf t
Router(config)# snmp-server community SECro ro 192.168.103.34
Router(config)# snmp-server host 192.168.103.34 SECtrap
Router(config)# snmp-server enable traps snmp linkdown linkup coldstart warmstart
```

2. Test SNMP access to the Cisco device

```
# snmpget -v 1 -c SECro 192.168.203.4 SNMPv2-MIB::sysDescr.0
SNMPv2-MIB::sysDescr.0 = STRING: Cisco Internetwork Operating System Software IOS (tm) C2950
Software (C2950-I6Q4L2-M), Version 12.1(22)EA9, RELEASE SOFTWARE (fc1) Copyright (c) 1986-2006
by cisco Systems, Inc. Compiled Fri 01-Dec-06 18:02 by weiliu
```

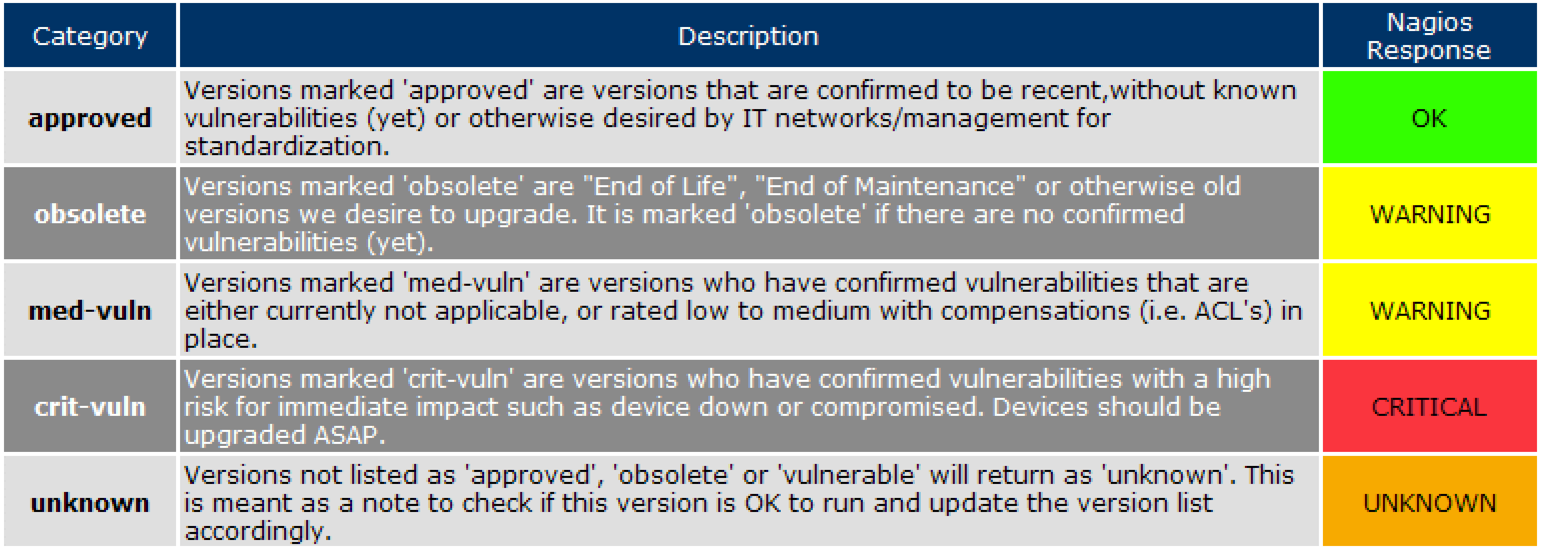
Cisco:
Router
Switches
FW's

Network devices are usually the best/most "monitored" systems for uptime/performance

They are already set up in Nagios, aren't they?

Patch monitoring: Cisco IOS, ASA, PIX – Nagios Setup

1. Cisco plugin – version compliance check categories



Category	Description	Nagios Response
approved	Versions marked 'approved' are versions that are confirmed to be recent,without known vulnerabilities (yet) or otherwise desired by IT networks/management for standardization.	OK
obsolete	Versions marked 'obsolete' are "End of Life", "End of Maintenance" or otherwise old versions we desire to upgrade. It is marked 'obsolete' if there are no confirmed vulnerabilities (yet).	WARNING
med-vuln	Versions marked 'med-vuln' are versions who have confirmed vulnerabilities that are either currently not applicable, or rated low to medium with compensations (i.e. ACL's) in place.	WARNING
crit-vuln	Versions marked 'crit-vuln' are versions who have confirmed vulnerabilities with a high risk for immediate impact such as device down or compromised. Devices should be upgraded ASAP.	CRITICAL
unknown	Versions not listed as 'approved', 'obsolete' or 'vulnerable' will return as 'unknown'. This is meant as a note to check if this version is OK to run and update the version list accordingly.	UNKNOWN

Nagios

IT SECURITY PATCH MONITORING WITH NAGIOS

```
/srv/app/nagios/etc/objects # vi check_snmp_patchlevel.cfg
# Below are the 'approved' versions we explicitly endorse for usage: #
######################################################################
approved|ios|12.2(13)ZH2|not OK, but currently being actively upgraded
# Below are the 'obsolete' versions we explicitly disapprove of:     #
######################################################################
obsolete|pix|7.2(2)|end-of-maintenance 2009-07-28
obsolete|ios|12.2(25)SEE4|end-of-maintenance date 2007-12-12
# Below are the 'med-vuln' versions with low to medium criticality   #
######################################################################
med-vuln|ios|12.4(6)T8|multiple DOS confirmed (Voice, Stack)
######################################################################
```

2. Cisco plugin – compliance check configuration file

Patch monitoring: Cisco IOS, ASA, PIX – Nagios Setup

1. Get, install and test the ‘check_snmp_patchlevel.pl’ script as a plugin

```
/srv/app/nagios/libexec # ./snmp_patchlevel.pl -H 192.168.203.4 -g ios -C SECro

IOS Version: 12.1(22)EA9 | Cisco Internetwork Operating System Software IOS (tm) C2950 Software
(C2950-I6Q4L2-M), Version 12.1(22)EA9, RELEASE SOFTWARE (fc1) Copyright (c) 1986-2006 by cisco
Systems, Inc. Compiled Fri 01-Dec-06 18:02 by weiliu
```

2. Configure the new plugin in the Nagios command.cfg section

```
/srv/app/nagios/etc/objects # vi commands.cfg

define command{
  command_name check_snmp_cisco_ios
  command_line $USER1$/check_snmp_patchlevel.pl -H $HOSTADDRESS$ -g ios -C $ARG1$
}

define command{
  command_name check_snmp_cisco_asa
  command_line $USER1$/check_snmp_patchlevel.pl -H $HOSTADDRESS$ -g asa -C $ARG1$
}
```

Nagios

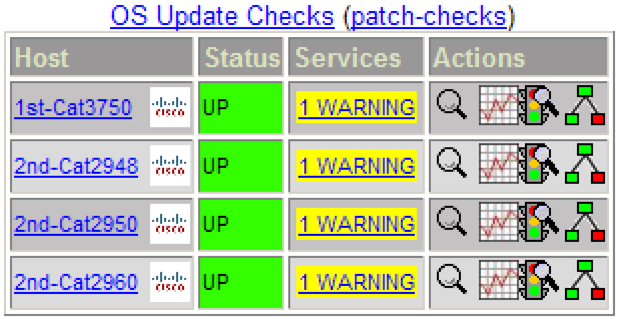
IT SECURITY PATCH MONITORING WITH NAGIOS

3. Configure the new patch monitoring service

```
/srv/app/nagios/etc/objects # vi sles10-patch-services.cfg

###############################################################################
# Check Cisco Router IOS version against a config file
###############################################################################
define service {
  use generic-patch
  hostgroup cisco-routers
  name check_snmp_ios_router
  service_description check_snmp_ios_router
  check_command check_snmp_cisco_ios!SECro
}
```

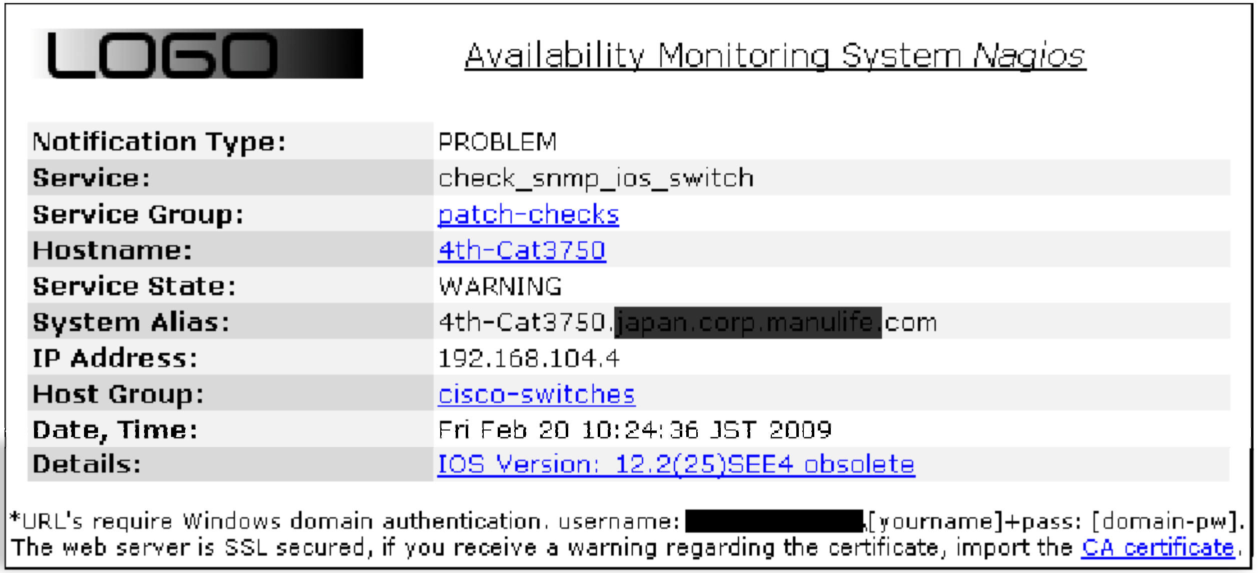
Patch monitoring: Cisco IOS, ASA, PIX – Nagios Views



OS Update Checks (patch-checks)

Host	Status	Services	Actions
1st-Cat3750	UP	1 WARNING	
2nd-Cat2948	UP	1 WARNING	
2nd-Cat2950	UP	1 WARNING	
2nd-Cat2960	UP	1 WARNING	

Service View and
E-Mail Notification

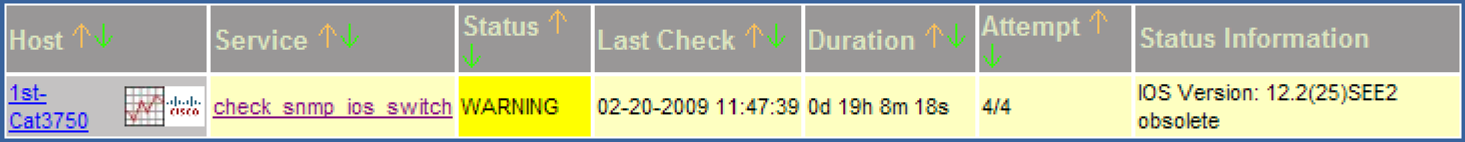


LOGO Availability Monitoring System *Nagios*

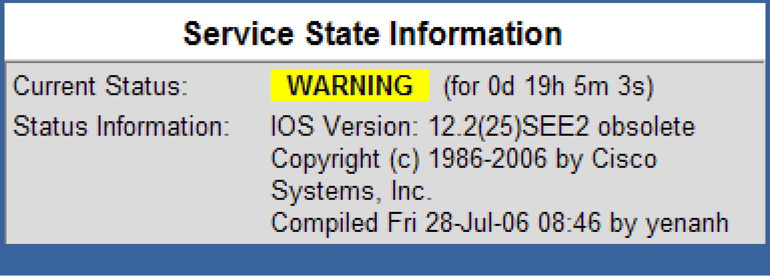
Notification Type:	PROBLEM
Service:	check_snmp_ios_switch
Service Group:	patch-checks
Hostname:	4th-Cat3750
Service State:	WARNING
System Alias:	4th-Cat3750.[redacted].com
IP Address:	192.168.104.4
Host Group:	cisco-switches
Date, Time:	Fri Feb 20 10:24:36 JST 2009
Details:	IOS Version: 12.2(25)SEE4 obsolete

*URL's require Windows domain authentication. username: [redacted][yourname]+pass: [domain-pw].
The web server is SSL secured, if you receive a warning regarding the certificate, import the CA certificate.

IT SECURITY PATCH MONITORING WITH NAGIOS



Host ↑↓	Service ↑↓	Status ↑↓	Last Check ↑↓	Duration ↑↓	Attempt ↑↓	Status Information
1st-Cat3750	check_snmp_ios_switch	WARNING	02-20-2009 11:47:39	0d 19h 8m 18s	4/4	IOS Version: 12.2(25)SEE2 obsolete



Service State Information

Current Status:	WARNING (for 0d 19h 5m 3s)
Status Information:	IOS Version: 12.2(25)SEE2 obsolete Copyright (c) 1986-2006 by Cisco Systems, Inc. Compiled Fri 28-Jul-06 08:46 by yenanh

3. Experience and Future

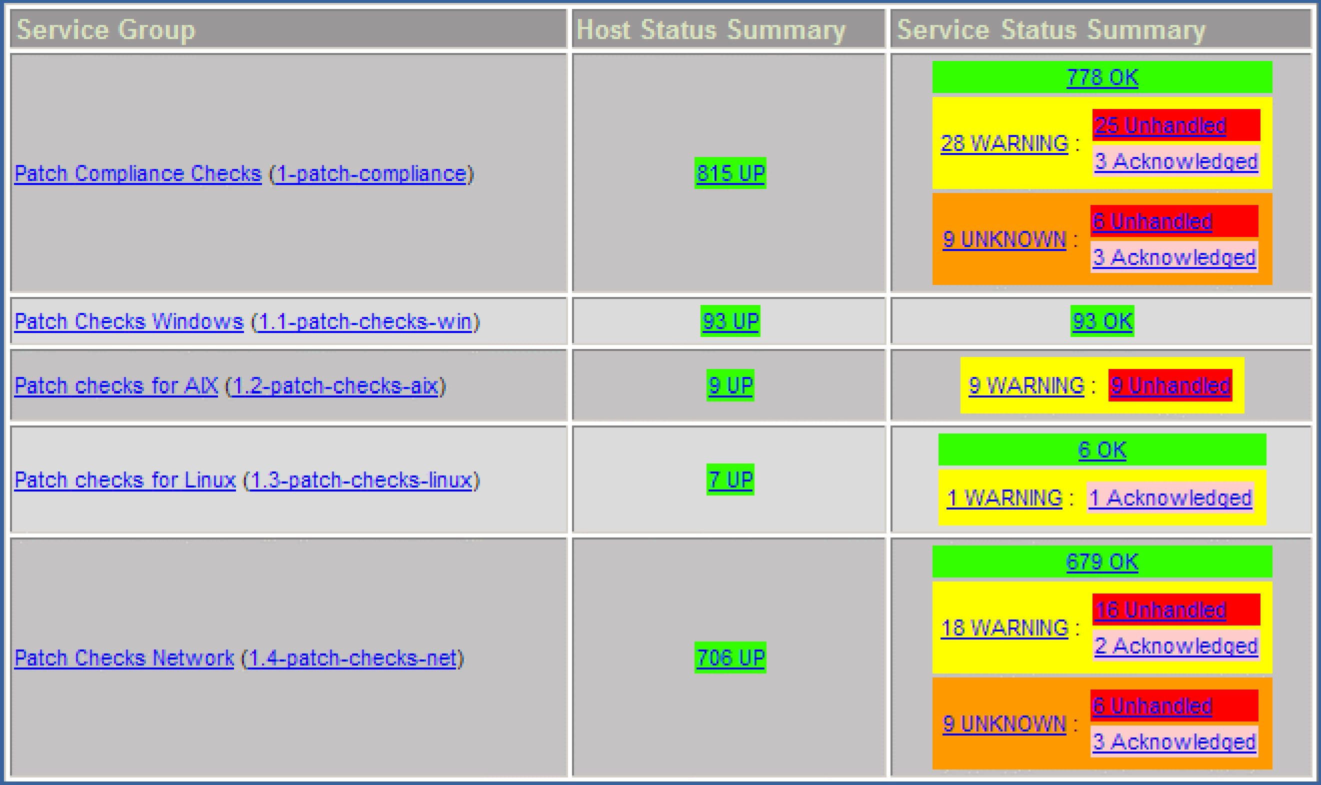
IT SECURITY PATCH MONITORING WITH NAGIOS

Frank Migge, Manager Information Security Office

OPEN SOURCE MONITORING CONFERENCE on Nagios

Formerly known as "Nagios Konferenz"

Central patch status view in Nagios



Service Group	Host Status Summary	Service Status Summary
Patch Compliance Checks (1-patch-compliance)	815 UP	778 OK 28 WARNING : 25 Unhandled 3 Acknowledged 9 UNKNOWN : 6 Unhandled 3 Acknowledged
Patch Checks Windows (1.1-patch-checks-win)	93 UP	93 OK
Patch checks for AIX (1.2-patch-checks-aix)	9 UP	9 WARNING : 9 Unhandled
Patch checks for Linux (1.3-patch-checks-linux)	7 UP	6 OK 1 WARNING : 1 Acknowledged
Patch Checks Network (1.4-patch-checks-net)	706 UP	679 OK 18 WARNING : 16 Unhandled 2 Acknowledged 9 UNKNOWN : 6 Unhandled 3 Acknowledged

IT SECURITY PATCH MONITORING WITH NAGIOS

Monitoring Patch Policy Compliance:

- open, outstanding patches
- time periods until patched
- current OS versions and patch update settings

Patch monitoring Issues and Improvements

Windows: Improving patch identification for WSUS managed systems

- Can we switch safely from WSUS to Windows Online and back to WSUS

Cisco: Automate the manual process to identify available updates

- Investigate the Cisco IOS Auto-Upgrade Manager, parse the Cisco Website with CCO credentials?

Expand patch and version monitoring into the applications space:

- First target major DB vendors: IBM, Oracle, Microsoft
  - Combine the "DB up" check with a DB real login and return the DB version using JAVA thinclients

Thank you for listening.

Time for Questions?