Discovered Systems

- **Repository :** Active
- **Asset List :** Lab Environment

|IP|Operating System|Risk|Low|Medium|High|Critical| |:-|:---------------|:---|:--|:-----|:---|:-------| |172.26.0.43|Mac OS X 10.4|59|3|2|1|1| |172.26.0.64|HP-UX B.11.11|28|2|2|2|0| |172.26.0.65|AIX 7.1|28|2|2|2|0| |172.26.0.66|Solaris 11|8|5|1|0|0| |172.26.0.68|Solaris 10 (sparc)|65|6|13|2|0| |172.26.0.204|Microsoft Windows Server 2008 R2 Standard Service Pack 1|30|8|4|1|0| |172.26.0.217|Mac OS X 10.8.3|118|2|2|11|0| |172.26.3.229|Linux Kernel 2.4 on Red Hat Enterprise Linux 3|33|3|10|0|0| |172.26.3.235|Linux Kernel 2.6|15|3|4|0|0| |172.26.3.236|Linux Kernel 2.6|15|3|4|0|0| |172.26.3.237|Linux Kernel 2.6|15|3|4|0|0| |172.26.16.17|Linux Kernel 2.6.18-308.20.1.el5 on Red Hat Enterprise Linux Server release 5.8 (Tikanga)|198|2|22|5|2| |172.26.16.32|Microsoft Windows Server 2008 R2 Datacenter Service Pack 1|37|12|5|1|0| |172.26.16.62| Linux Kernel 2.6 PelcoLinux|47|6|7|2|0| |172.26.17.8|Microsoft Windows Server 2008 R2 Standard Service Pack 1|30|8|4|1|0| |172.26.17.9|Microsoft Windows Server 2008 R2 Standard Service Pack 1|30|8|4|1|0| |172.26.17.10|Microsoft Windows Server 2008 R2 Enterprise Service Pack 1|31|6|5|1|0| |172.26.17.11|Microsoft Windows Server 2008 R2 Datacenter Service Pack 1|34|12|4|1|0| |172.26.17.60|Linux Kernel 2.6.18-308.20.1.el5 on Red Hat Enterprise Linux Server release 5.8 (Tikanga)|202|3|23|5|2| |172.26.17.61|Linux Kernel 2.6.18-308.20.1.el5 on Red Hat Enterprise Linux Server release 5.8 (Tikanga)|202|3|23|5|2| |172.26.17.63|Linux Kernel 2.6.18-308.13.1.el5 on Red Hat Enterprise Linux Server release 5.8 (Tikanga)|427|3|28|10|6| |172.26.17.69| Linux Kernel 2.6 on Fedora 13 Linux Kernel 2.6 on Fedora 14 Linux Kernel 2.6 on Fedora 15|47|6|7|2|0| |172.26.17.110|Microsoft Windows XP|524|2|4|3|12| |172.26.17.111|Microsoft Windows XP|350|1|3|2|8| |172.26.17.129|Microsoft Windows 7 Ultimate|24|2|4|1|0| |172.26.17.230|Microsoft Windows Server 2008 Standard Service Pack 1|31|9|4|1|0| |172.26.17.231| Microsoft Windows XP Service Pack 2 Microsoft Windows XP Service Pack 3|214|9|5|3|4| |172.26.17.242|Linux Kernel 2.6.27.7-smp|26|3|1|2|0| |172.26.20.25|Linux Kernel 2.6|9|3|2|0|0| |172.26.20.71|Microsoft Windows Server 2008 Standard Service Pack 1|27|2|5|1|0| |172.26.20.73|Microsoft Windows Server 2008 Standard Service Pack 1|27|2|5|1|0| |172.26.20.151|Microsoft Windows Server 2008 R2 Enterprise Service Pack 1|28|9|3|1|0| |172.26.20.155| Linux Kernel 2.4 Linux Kernel 2.6|30|5|5|1|0| |172.26.20.182|Microsoft Windows Server 2008 R2 Standard Service Pack 1|24|2|4|1|0| |172.26.21.100| Linux Kernel 2.6 PelcoLinux|26|5|7|0|0| |172.26.21.112|Linux Kernel 2.6|18|6|4|0|0| |172.26.22.1| Microsoft Windows XP Service Pack 2 Microsoft Windows XP Service Pack 3|109|1|6|1|2| |172.26.22.15| Microsoft Windows XP Service Pack 2 Microsoft Windows XP Service Pack 3|81|1|10|1|1| |172.26.22.23|Microsoft Windows XP Professional|14|1|1|1|0| |172.26.22.25| Microsoft Windows XP Service Pack 2 Microsoft Windows XP Service Pack 3|193|1|4|2|4| |172.26.22.32| Linux Kernel 3.5 Linux Kernel 3.8|15|2|1|1|0| |172.26.22.34| Linux Kernel 3.5 Linux Kernel 3.8|22|6|2|1|0| |172.26.22.35|Microsoft Windows Server 2008 Enterprise Service Pack 2|19|7|4|0|0| |172.26.22.41|Microsoft Windows Server 2003 Service Pack 2|132|10|4|3|2| |172.26.22.46|Microsoft Windows Server 2008 R2 Enterprise Service Pack 1|48|10|6|2|0| |172.26.22.51|VMware ESX 4.1.0|14|1|1|1|0| |172.26.22.55|Microsoft Windows Server 2008 R2 Enterprise Service Pack 1|19|3|2|1|0| |172.26.22.60|Linux Kernel 3.5 on Ubuntu 12.10 (quantal)|4|1|1|0|0| |172.26.22.67|Linux Kernel 2.6|15|3|4|0|0| |172.26.22.76|Linux Kernel 2.6|9|3|2|0|0| |172.26.22.82|Microsoft Windows Server 2008 Standard Service Pack 1|166|8|6|2|3| |172.26.22.100|Microsoft Windows Server 2003 Service Pack 2|30|12|6|0|0| |172.26.22.104|Microsoft Windows Server 2008 Enterprise Service Pack 2|48|11|9|1|0| |172.26.22.108|Microsoft Windows Server 2003 Service Pack 2|413|7|12|13|6| |172.26.22.109|Microsoft Windows Server 2008 R2 Enterprise Service Pack 1|69|7|4|1|1| |172.26.22.113|Linux Kernel 2.6.18-194.3.1.el5 (x86*64)|133|3|0|1|3| |172.26.22.117|*Microsoft Windows Server 2003 Service Pack 2|109|7|4|1|2|* |172.26.22.134|*Microsoft Windows Server 2008 R2 Standard Service Pack 1|63|1|4|1|1|* | 172.26.22.151| *Microsoft Windows XP Service Pack 2 Microsoft Windows XP Service Pack 3|87|2|15|0|1|* |172.26.22.156|*Microsoft Windows Server 2003 Service Pack 2|23|1|4|1|0|* |172.26.22.195|*Linux Kernel 2.6 on Ubuntu 10.04 (lucid)|107|2|25|3|0|* |172.26.22.211| *Linux Kernel 3.5 Linux Kernel 3.8|4|1|1|0|0|* | 172.26.22.212|*Microsoft Windows Server 2008 R2 Enterprise Service Pack 1|90|1|13|1|1|* |172.26.22.219|*Linux Kernel 2.6|78|9|3|2|1|* | 172.26.22.221|*Linux Kernel 2.6|85|10|5|2|1|* |172.26.22.222|*Linux Kernel 2.6|22|4|6|0|0|* | 172.26.22.240|*Microsoft Windows Server 2008 R2 Enterprise Service Pack 1|16|0|2|1|0|* |172.26.22.241|*Microsoft Windows 7 Ultimate|67|8|3|1|1|* | 172.26.22.248|*Microsoft Windows Vista Ultimate|103|1|4|1|2|* |172.26.22.249| *Microsoft Windows XP Service Pack 2 Microsoft Windows XP Service Pack 3|193|1|4|2|4|* |172.26.22.250| *Microsoft Windows 7 Microsoft Windows 8 Microsoft Windows Server 2008 Microsoft Windows Server 2012 Microsoft Windows Vista|20|1|3|1|0|* |172.26.22.251|*Microsoft Windows Server 2008 Standard Service Pack 1|103|1|4|1|2|* |172.26.22.252|*Microsoft Windows Server 2003 Service Pack 2|103|1|4|1|2|* | 172.26.23.13|*Microsoft Windows Server 2008 R2 Datacenter Service Pack 1|359|2|9|29|1|* |172.26.23.18|*Microsoft Windows Server 2008 R2 Datacenter Service Pack 1|214|2|4|16|1|* |172.26.23.27|*Microsoft Windows Server 2008 R2 Datacenter Service Pack 1|319|1|6|26|1|* |172.26.23.33|*Microsoft Windows Server 2008 R2 Datacenter Service Pack 1|337|4|11|26|1|* | 172.26.23.41|*Microsoft Windows Server 2008 R2 Datacenter Service Pack 1|757|3|8|69|1|* |172.26.23.43|*Microsoft Windows Server 2008 R2 Datacenter Service Pack 1|331|3|6|27|1|* |172.26.23.62|*Microsoft Windows Server 2008 R2 Datacenter Service Pack 1|154|2|4|14|0|* |172.26.23.73|*Microsoft Windows Server 2008 R2 Datacenter Service Pack 1|320|2|6|26|1|* | 172.26.23.83|*Microsoft Windows XP|20|1|3|1|0|* |172.26.23.105|*Solaris 10 (i386)|79|4|5|2|1|* |172.26.23.107|*Microsoft Windows Server 2003 Service Pack 2|93|1|4|0|2|* |172.26.23.112|*Linux Kernel 2.6|7|1|2|0|0|* | 172.26.23.117|*Microsoft Windows Server 2003 Service Pack 2|93|1|4|0|2|* |172.26.23.128|*Microsoft Windows Server 2003 Service Pack 2|93|1|4|0|2|* | 172.26.23.131|*Linux Kernel 2.6 on Ubuntu 10.04 (lucid)|38|4|8|1|0|* |172.26.23.138|*Linux Kernel 2.6.18-274.el5|106|4|4|1|2|* | 172.26.23.145|*Microsoft Windows Server 2008 R2 Datacenter Service Pack 1|322|1|7|26|1|* |172.26.23.157|*Microsoft Windows Server 2003 Service Pack 2|93|1|4|0|2|* |172.26.23.158|*Microsoft Windows 7 Ultimate|47|3|8|2|0|* | 172.26.23.165|*Linux Kernel 2.6.18-194.3.1.el5|213|3|0|1|5|* |172.26.23.170|*Microsoft Windows Server 2003 Service Pack 2|93|1|4|0|2|* | 172.26.23.173| *Linux Kernel 2.4 Linux Kernel 2.6|19|1|6|0|0|* |172.26.23.182|*Microsoft Windows Server 2008 R2 Enterprise Service Pack 1|16|0|2|1|0|* |172.26.23.186|*Microsoft Windows Server 2008 R2 Enterprise Service Pack 1|65|3|4|1|1|* | 172.26.23.188| *Linux

*Kernel 2.4 Linux Kernel 2.6|19|1|6|0|0| |172.26.32.135|Microsoft Windows Server 2003 Service Pack 2|64|3|17|1|0| |172.26.32.214| Linux Kernel 3.5 Linux Kernel 3.8|36|8|6|1|0| | 172.26.33.234|Microsoft Windows 7 Ultimate|53|10|11|1|0| |172.26.34.30|Linux Kernel 3.5 on Ubuntu 12.10 (quantal)|69|0|3|2|1| | 172.26.34.184| Linux Kernel 3.2 Linux Kernel 3.3|12|9|1|0|0| |172.26.48.26|Linux Kernel 2.6.26-2-686 on Debian 5.0.2|625|2|31|29|6| |172.26.48.28|Linux Kernel 2.6.11-1.1369*FC4 on Fedora Core release 4 (Stentz)|660|7|11|54|2| |172.26.48.31|Linux Kernel 2.6.23.12-52.fc7 on Fedora release 7 (Moonshine)|327|2|15|8|5| |172.26.48.45|Linux Kernel 2.4.21-53.EL on Red Hat Enterprise Linux ES release 3 (Taroon Update 9)|728|0|36|22|10| |172.26.48.46|Linux Kernel 2.6.9-67.0.1.ELsmp on Red Hat Enterprise Linux ES release 4 (Nahant Update 6)|1429|1|56|62|16| |172.26.48.47|Linux Kernel 2.6.9-67.0.1.EL on Red Hat Enterprise Linux ES release 4 (Nahant Update 6)|1425|0|55|62|16| |172.26.48.48|Linux Kernel 2.6.9-67.0.1.EL on Red Hat Enterprise Linux ES release 4 (Nahant Update 6)|1425|0|55|62|16| |172.26.48.49|Linux Kernel 2.6.9-67.0.1.EL on Red Hat Enterprise Linux ES release 4 (Nahant Update 6)|1422|0|54|62|16| |172.26.48.50|Linux Kernel 2.6.18-128.el5 on Red Hat Enterprise Linux Server release 5.3 (Tikanga)|3434|14|160|138|39| |172.26.48.51|Linux Kernel 2.6.18-128.el5 on Red Hat Enterprise Linux Server release 5.3 (Tikanga)|3220|14|142|130|37| |172.26.48.52|Linux Kernel 2.6.32-71.el6.i686 on Red Hat Enterprise Linux Server release 6.0 (Santiago)|1859|10|113|67|21| |172.26.48.53|Linux Kernel 2.6.32-71.el6.x86*64 on Red Hat Enterprise Linux Server release 6.0 (Santiago)|2534|15|133|88|31| |172.26.48.58|Linux Kernel 2.6.28-11-server on Ubuntu 9.04|1104|2|44|29|17| |172.26.48.59|Linux Kernel 2.6.28-11-server on Ubuntu 9.04|863|3|40|26|12| | 172.26.48.61|Linux Kernel 2.6.38-8-generic-pae on Ubuntu 11.04|539|2|29|29|4| |172.26.48.64|Microsoft Windows Server 2003 Service Pack 2|328|17|27|11|3| |172.26.48.68| Microsoft Windows 2000 Server Microsoft Windows XP Professional|27|11|2|1|0| | 172.26.48.69| Microsoft Windows 2000 Server Microsoft Windows XP Professional|27|11|2|1|0| |172.26.48.71|Microsoft Windows XP Professional|357|13|8|12|5| |172.26.48.72|Microsoft Windows Vista Ultimate|64|2|4|1|1| |172.26.48.73|Microsoft Windows Vista Ultimate|64|2|4|1|1| |172.26.48.74|Microsoft Windows 7 Ultimate|23|1|4|1|0| |172.26.48.75|Microsoft Windows 7 Ultimate|33|2|7|1|0| |172.26.48.78|Linux Kernel 2.6.32-279.5.2.el6.x86*64 on CentOS release 6.3 (Final)|430|4|32|13|5| |172.26.48.79|Linux Kernel 2.6.32-279.5.2.el6.x86*64 on CentOS release 6.3 (Final)|427|4|31|13|5| |172.26.48.82|VMware ESXi|14|1|1|1|0| |172.26.48.84|Mac OS X 10.6.8|295|2|1|25|1| |172.26.48.85|Mac OS X 10.7.5|18|2|2|1|0| |172.26.48.86|Mac OS X 10.8.3|11|1|0|1|0| |172.26.48.89| Microsoft Windows 7 Microsoft Windows 8 Microsoft Windows Server 2008 Microsoft Windows Server 2012 Microsoft Windows Vista|21|2|3|1|0| |172.26.51.154|Microsoft Windows 2000 Server Service Pack 4|461|3|6|4|10| |172.26.246.101|Linux Kernel 2.6.18-194.el5 (x86* 64)|41|1|0|0|1| |172.26.246.102|Linux Kernel 2.6.18-194.el5 (x86*64)|41|1|0|0|1| |172.26.246.103|Linux Kernel 2.6.18-194.el5 (x86* 64)|41|1|0|0|1| |172.26.246.104|Linux Kernel 2.6.18-194.el5 (x86_64)|41|1|0|0|1|

Remediation Plan

Remediation Plan for 172.26.0.43

You need to take the following 1 actions:

- Apache HTTP Server httpOnly Cookie Information Disclosure (57792):
  - Upgrade to Apache version 2.2.22 or later.

Remediation Plan for 172.26.0.64

You need to take the following 1 actions:

- Multiple Mail Server EXPN/VRFY Information Disclosure (10249):
  - If you are using Sendmail, add the option : O PrivacyOptions=goaway in /etc/sendmail.cf.

Remediation Plan for 172.26.0.65

You need to take the following 1 actions:

- Multiple Mail Server EXPN/VRFY Information Disclosure (10249):
  - If you are using Sendmail, add the option : O PrivacyOptions=goaway in /etc/sendmail.cf.

Remediation Plan for 172.26.0.66

You need to take the following 1 actions:

- Apache HTTP Server httpOnly Cookie Information Disclosure (57792):
  - Upgrade to Apache version 2.2.22 or later.

Remediation Plan for 172.26.0.68

You need to take the following 1 actions:

- Multiple Mail Server EXPN/VRFY Information Disclosure (10249):
  - If you are using Sendmail, add the option : O PrivacyOptions=goaway in /etc/sendmail.cf.

Remediation Plan for 172.26.0.204

You need to take the following 1 actions:

- MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check) (58435):
  - Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 : http://technet.microsoft.com/en-us/security/bulletin/ms12-020

Remediation Plan for 172.26.0.217

You need to take the following 5 actions:

- Adobe Reader < 11.0.2 / 10.1.6 / 9.5.4 Multiple Vulnerabilities (APSB13-07) (Mac OS X) (64787):
  - Upgrade to Adobe Reader 11.0.2 / 10.1.6 / 9.5.4 or later.
- Firefox ESR 17.x < 17.0.5 Multiple Vulnerabilities (Mac OS X) (65801):
  - Upgrade to Firefox 17.0.5 ESR or later.
- Thunderbird ESR 17.x < 17.0.5 Multiple Vulnerabilities (Mac OS X) (65804):
  - Upgrade to Thunderbird ESR 17.0.5 or later.
- Mac OS X : Java for OS X 2013-003 (65999):
  - Apply the Java for OS X 2013-003 update, which includes version 14.7.0 of the JavaVM Framework.
- Mac OS X : Safari < 6.0.4 SVG File Handling Arbitrary Code Execution (66000):
  - Upgrade to Safari 6.0.4 or later.

Remediation Plan for 172.26.3.229

You need to take the following 2 actions:

- OpenSSL SSL*OP*NETSCAPE*REUSE*CIPHER*CHANGE*BUG Session Resume Ciphersuite Downgrade Issue (51892):
  - Upgrade to OpenSSL 0.9.8q / 1.0.0.c or later, or contact your vendor for a patch.
- Apache HTTP Server httpOnly Cookie Information Disclosure (57792):
  - Upgrade to Apache version 2.2.22 or later.

Remediation Plan for 172.26.3.235

You need to take the following 1 actions:

- Apache HTTP Server httpOnly Cookie Information Disclosure (57792):
  - Upgrade to Apache version 2.2.22 or later.

Remediation Plan for 172.26.3.236

You need to take the following 1 actions:

- Apache HTTP Server httpOnly Cookie Information Disclosure (57792):
  - Upgrade to Apache version 2.2.22 or later.

Remediation Plan for 172.26.3.237

You need to take the following 1 actions:

- Apache HTTP Server httpOnly Cookie Information Disclosure (57792):
  - Upgrade to Apache version 2.2.22 or later.

Remediation Plan for 172.26.16.17

You need to take the following 23 actions:

- RHEL 5 / 6 : libtiff (RHSA-2012-1590) (63293):
  - Update the affected packages.
- RHEL 5 : quota (RHSA-2013-0120) (63403):
  - Update the affected quota package.
- RHEL 5 : tcl (RHSA-2013-0122) (63405):
  - Update the affected tcl, tcl-devel and / or tcl-html packages.
- RHEL 5 : OpenIPMI (RHSA-2013-0123) (63406):
  - Update the affected packages.

- RHEL 5 : net-snmp (RHSA-2013-0124) (63407):
  - Update the affected packages.
- RHEL 5 : gnome-vfs2 (RHSA-2013-0131) (63412):
  - Update the affected gnome-vfs2, gnome-vfs2-devel and / or gnome-vfs2-smb packages.
- RHEL 5 : autofs (RHSA-2013-0132) (63413):
  - Update the affected autofs package.
- RHEL 5 : gtk2 (RHSA-2013-0135) (63416):
  - Update the affected gtk2 and / or gtk2-devel packages.
- RHEL 5 / 6 : firefox (RHSA-2013-0144) (63445):
  - Update the affected packages.
- RHEL 5 / 6 : freetype (RHSA-2013-0216) (64390):
  - Update the affected packages.
- RHEL 5 / 6 : elinks (RHSA-2013-0250) (64565):
  - Update the affected elinks and / or elinks-debuginfo packages.
- RHEL 5 / 6 : firefox (RHSA-2013-0271) (64696):
  - Update the affected packages.
- RHEL 5 / 6 : dbus-glib (RHSA-2013-0568) (64904):
  - Update the affected dbus-glib, dbus-glib-debuginfo and / or dbus-glib-devel packages.
- RHEL 5 / 6 : cups (RHSA-2013-0580) (64944):
  - Update the affected packages.
- RHEL 5 / 6 : libxml2 (RHSA-2013-0581) (64945):
  - Update the affected packages.
- RHEL 5 / 6 : openssl (RHSA-2013-0587) (65004):
  - Update the affected packages.
- RHEL 5 / 6 : gnutls (RHSA-2013-0588) (65005):
  - Update the affected packages.
- RHEL 5 / 6 : boost (RHSA-2013-0668) (65651):
  - Update the affected packages.
- RHEL 5 / 6 : perl (RHSA-2013-0685) (65698):
  - Update the affected packages.
- RHEL 5 / 6 : subversion (RHSA-2013-0737) (65938):
  - Update the affected packages.
- RHEL 5 : kernel (RHSA-2013-0747) (65991):
  - Update the affected packages.
- RHEL 5 : glibc (RHSA-2013-0769) (66211):
  - Update the affected packages.
- RHEL 5 / 6 : curl (RHSA-2013-0771) (66213):
  - Update the affected packages.

Remediation Plan for 172.26.16.32

You need to take the following 1 actions:

- MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check) (58435):
  - Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 : http://technet.microsoft.com/en-us/security/bulletin/ms12-020

Remediation Plan for 172.26.16.62

You need to take the following 1 actions:

- Apache HTTP Server httpOnly Cookie Information Disclosure (57792):
  - Upgrade to Apache version 2.2.22 or later.

Remediation Plan for 172.26.17.8

You need to take the following 1 actions:

- MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check) (58435):
  - Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 : http://technet.microsoft.com/en-us/security/bulletin/ms12-020

Remediation Plan for 172.26.17.9

You need to take the following 1 actions:

- MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check) (58435):
    - Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 : http://technet.microsoft.com/en-us/security/bulletin/ms12-020

Remediation Plan for 172.26.17.10

You need to take the following 1 actions:

- MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check) (58435):
    - Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 : http://technet.microsoft.com/en-us/security/bulletin/ms12-020

Remediation Plan for 172.26.17.11

You need to take the following 1 actions:

- MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check) (58435):
    - Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 : http://technet.microsoft.com/en-us/security/bulletin/ms12-020

Remediation Plan for 172.26.17.60

You need to take the following 23 actions:

- RHEL 5 / 6 : libtiff (RHSA-2012-1590) (63293):
    - Update the affected packages.
- RHEL 5 : quota (RHSA-2013-0120) (63403):
    - Update the affected quota package.
- RHEL 5 : tcl (RHSA-2013-0122) (63405):
    - Update the affected tcl, tcl-devel and / or tcl-html packages.
- RHEL 5 : OpenIPMI (RHSA-2013-0123) (63406):
    - Update the affected packages.
- RHEL 5 : net-snmp (RHSA-2013-0124) (63407):
    - Update the affected packages.
- RHEL 5 : gnome-vfs2 (RHSA-2013-0131) (63412):
    - Update the affected gnome-vfs2, gnome-vfs2-devel and / or gnome-vfs2-smb packages.
- RHEL 5 : autofs (RHSA-2013-0132) (63413):
    - Update the affected autofs package.
- RHEL 5 : gtk2 (RHSA-2013-0135) (63416):
    - Update the affected gtk2 and / or gtk2-devel packages.
- RHEL 5 / 6 : firefox (RHSA-2013-0144) (63445):
    - Update the affected packages.
- RHEL 5 / 6 : freetype (RHSA-2013-0216) (64390):
    - Update the affected packages.
- RHEL 5 / 6 : elinks (RHSA-2013-0250) (64565):
    - Update the affected elinks and / or elinks-debuginfo packages.
- RHEL 5 / 6 : firefox (RHSA-2013-0271) (64696):
    - Update the affected packages.
- RHEL 5 / 6 : dbus-glib (RHSA-2013-0568) (64904):
    - Update the affected dbus-glib, dbus-glib-debuginfo and / or dbus-glib-devel packages.
- RHEL 5 / 6 : cups (RHSA-2013-0580) (64944):
    - Update the affected packages.
- RHEL 5 / 6 : libxml2 (RHSA-2013-0581) (64945):
    - Update the affected packages.
- RHEL 5 / 6 : openssl (RHSA-2013-0587) (65004):
    - Update the affected packages.
- RHEL 5 / 6 : gnutls (RHSA-2013-0588) (65005):
    - Update the affected packages.
- RHEL 5 / 6 : boost (RHSA-2013-0668) (65651):
    - Update the affected packages.
- RHEL 5 / 6 : perl (RHSA-2013-0685) (65698):
    - Update the affected packages.
- RHEL 5 / 6 : subversion (RHSA-2013-0737) (65938):
    - Update the affected packages.

- RHEL 5 : kernel (RHSA-2013-0747) (65991):
  - Update the affected packages.
- RHEL 5 : glibc (RHSA-2013-0769) (66211):
  - Update the affected packages.
- RHEL 5 / 6 : curl (RHSA-2013-0771) (66213):
  - Update the affected packages.

Remediation Plan for 172.26.17.61

You need to take the following 23 actions:

- RHEL 5 / 6 : libtiff (RHSA-2012-1590) (63293):
  - Update the affected packages.
- RHEL 5 : quota (RHSA-2013-0120) (63403):
  - Update the affected quota package.
- RHEL 5 : tcl (RHSA-2013-0122) (63405):
  - Update the affected tcl, tcl-devel and / or tcl-html packages.
- RHEL 5 : OpenIPMI (RHSA-2013-0123) (63406):
  - Update the affected packages.
- RHEL 5 : net-snmp (RHSA-2013-0124) (63407):
  - Update the affected packages.
- RHEL 5 : gnome-vfs2 (RHSA-2013-0131) (63412):
  - Update the affected gnome-vfs2, gnome-vfs2-devel and / or gnome-vfs2-smb packages.
- RHEL 5 : autofs (RHSA-2013-0132) (63413):
  - Update the affected autofs package.
- RHEL 5 : gtk2 (RHSA-2013-0135) (63416):
  - Update the affected gtk2 and / or gtk2-devel packages.
- RHEL 5 / 6 : firefox (RHSA-2013-0144) (63445):
  - Update the affected packages.
- RHEL 5 / 6 : freetype (RHSA-2013-0216) (64390):
  - Update the affected packages.
- RHEL 5 / 6 : elinks (RHSA-2013-0250) (64565):
  - Update the affected elinks and / or elinks-debuginfo packages.
- RHEL 5 / 6 : firefox (RHSA-2013-0271) (64696):
  - Update the affected packages.
- RHEL 5 / 6 : dbus-glib (RHSA-2013-0568) (64904):
  - Update the affected dbus-glib, dbus-glib-debuginfo and / or dbus-glib-devel packages.
- RHEL 5 / 6 : cups (RHSA-2013-0580) (64944):
  - Update the affected packages.
- RHEL 5 / 6 : libxml2 (RHSA-2013-0581) (64945):
  - Update the affected packages.
- RHEL 5 / 6 : openssl (RHSA-2013-0587) (65004):
  - Update the affected packages.
- RHEL 5 / 6 : gnutls (RHSA-2013-0588) (65005):
  - Update the affected packages.
- RHEL 5 / 6 : boost (RHSA-2013-0668) (65651):
  - Update the affected packages.
- RHEL 5 / 6 : perl (RHSA-2013-0685) (65698):
  - Update the affected packages.
- RHEL 5 / 6 : subversion (RHSA-2013-0737) (65938):
  - Update the affected packages.
- RHEL 5 : kernel (RHSA-2013-0747) (65991):
  - Update the affected packages.
- RHEL 5 : glibc (RHSA-2013-0769) (66211):
  - Update the affected packages.
- RHEL 5 / 6 : curl (RHSA-2013-0771) (66213):
  - Update the affected packages.

Remediation Plan for 172.26.17.63

You need to take the following 28 actions:

- RHEL 5 / 6 : ghostscript (RHSA-2012-1256) (62056):
  - Update the affected packages.
- RHEL 5 : postgresql (RHSA-2012-1264) (62089):
  - Update the affected packages.
- RHEL 5 / 6 : libxslt (RHSA-2012-1265) (62090):
  - Update the affected packages.

- RHEL 5 / 6 : xulrunner (RHSA-2012-1361) (62541):
  - Update the affected xulrunner, xulrunner-debuginfo and / or xulrunner-devel packages.
- RHEL 5 / 6 : bind (RHSA-2012-1363) (62543):
  - Update the affected packages.
- RHEL 5 / 6 : libtiff (RHSA-2012-1590) (63293):
  - Update the affected packages.
- RHEL 5 : quota (RHSA-2013-0120) (63403):
  - Update the affected quota package.
- RHEL 5 : tcl (RHSA-2013-0122) (63405):
  - Update the affected tcl, tcl-devel and / or tcl-html packages.
- RHEL 5 : OpenIPMI (RHSA-2013-0123) (63406):
  - Update the affected packages.
- RHEL 5 : net-snmp (RHSA-2013-0124) (63407):
  - Update the affected packages.
- RHEL 5 : gnome-vfs2 (RHSA-2013-0131) (63412):
  - Update the affected gnome-vfs2, gnome-vfs2-devel and / or gnome-vfs2-smb packages.
- RHEL 5 : autofs (RHSA-2013-0132) (63413):
  - Update the affected autofs package.
- RHEL 5 : gtk2 (RHSA-2013-0135) (63416):
  - Update the affected gtk2 and / or gtk2-devel packages.
- RHEL 5 / 6 : firefox (RHSA-2013-0144) (63445):
  - Update the affected packages.
- RHEL 5 / 6 : freetype (RHSA-2013-0216) (64390):
  - Update the affected packages.
- RHEL 5 / 6 : elinks (RHSA-2013-0250) (64565):
  - Update the affected elinks and / or elinks-debuginfo packages.
- RHEL 5 / 6 : firefox (RHSA-2013-0271) (64696):
  - Update the affected packages.
- RHEL 5 / 6 : dbus-glib (RHSA-2013-0568) (64904):
  - Update the affected dbus-glib, dbus-glib-debuginfo and / or dbus-glib-devel packages.
- RHEL 5 / 6 : cups (RHSA-2013-0580) (64944):
  - Update the affected packages.
- RHEL 5 / 6 : libxml2 (RHSA-2013-0581) (64945):
  - Update the affected packages.
- RHEL 5 / 6 : openssl (RHSA-2013-0587) (65004):
  - Update the affected packages.
- RHEL 5 / 6 : gnutls (RHSA-2013-0588) (65005):
  - Update the affected packages.
- RHEL 5 / 6 : boost (RHSA-2013-0668) (65651):
  - Update the affected packages.
- RHEL 5 / 6 : perl (RHSA-2013-0685) (65698):
  - Update the affected packages.
- RHEL 5 / 6 : subversion (RHSA-2013-0737) (65938):
  - Update the affected packages.
- RHEL 5 : kernel (RHSA-2013-0747) (65991):
  - Update the affected packages.
- RHEL 5 : glibc (RHSA-2013-0769) (66211):
  - Update the affected packages.
- RHEL 5 / 6 : curl (RHSA-2013-0771) (66213):
  - Update the affected packages.

Remediation Plan for 172.26.17.69

You need to take the following 1 actions:

- Apache HTTP Server httpOnly Cookie Information Disclosure (57792):
  - Upgrade to Apache version 2.2.22 or later.

Remediation Plan for 172.26.17.110

You need to take the following 3 actions:

- MS05-027: Vulnerability in SMB Could Allow Remote Code Execution (896422) (uncredentialed check) (18502):
  - Microsoft has released a set of patches for Windows 2000, XP and 2003 : http://technet.microsoft.com/en-us/security/bulletin/ms05-027
- MS05-051: Vulnerabilities in MSDTC Could Allow Remote Code Execution (902400) (uncredentialed check) (20008):
  - Microsoft has released a set of patches for Windows 2000, XP and 2003 : http://technet.microsoft.com/en-us/security/bulletin/ms05-051

- MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check) (58435):
    - Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 : http://technet.microsoft.com/en-us/security/bulletin/ms12-020

Remediation Plan for 172.26.17.111

You need to take the following 1 actions:

- MS05-027: Vulnerability in SMB Could Allow Remote Code Execution (896422) (uncredentialed check) (18502):
    - Microsoft has released a set of patches for Windows 2000, XP and 2003 : http://technet.microsoft.com/en-us/security/bulletin/ms05-027

Remediation Plan for 172.26.17.129

You need to take the following 1 actions:

- MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check) (58435):
    - Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 : http://technet.microsoft.com/en-us/security/bulletin/ms12-020

Remediation Plan for 172.26.17.230

You need to take the following 1 actions:

- MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check) (58435):
    - Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 : http://technet.microsoft.com/en-us/security/bulletin/ms12-020

Remediation Plan for 172.26.17.231

You need to take the following 3 actions:

- MySQL Unpassworded Account Check (10481):
    - Disable or set a password for the affected account.
- MS05-027: Vulnerability in SMB Could Allow Remote Code Execution (896422) (uncredentialed check) (18502):
    - Microsoft has released a set of patches for Windows 2000, XP and 2003 : http://technet.microsoft.com/en-us/security/bulletin/ms05-027
- MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check) (58435):
    - Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 : http://technet.microsoft.com/en-us/security/bulletin/ms12-020

Remediation Plan for 172.26.17.242

You need to take the following 1 actions:

- Apache HTTP Server httpOnly Cookie Information Disclosure (57792):
    - Upgrade to Apache version 2.2.22 or later.

Remediation Plan for 172.26.20.25

You need to take the following 1 actions:

- Apache HTTP Server httpOnly Cookie Information Disclosure (57792):
    - Upgrade to Apache version 2.2.22 or later.

Remediation Plan for 172.26.20.71

You need to take the following 1 actions:

- MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check) (58435):
    - Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 : http://technet.microsoft.com/en-us/security/bulletin/ms12-020

Remediation Plan for 172.26.20.73

You need to take the following 1 actions:

- MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check) (58435):
    - Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 : http://technet.microsoft.com/en-us/security/bulletin/ms12-020

Remediation Plan for 172.26.20.151

You need to take the following 1 actions:

- MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check) (58435):
    - Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 : http://technet.microsoft.com/en-us/security/bulletin/ms12-020

Remediation Plan for 172.26.20.155

You need to take the following 1 actions:

- Apache HTTP Server httpOnly Cookie Information Disclosure (57792):
    - Upgrade to Apache version 2.2.22 or later.

Remediation Plan for 172.26.20.182

You need to take the following 1 actions:

- MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check) (58435):
    - Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 : http://technet.microsoft.com/en-us/security/bulletin/ms12-020

Remediation Plan for 172.26.21.100

You need to take the following 1 actions:

- Apache HTTP Server httpOnly Cookie Information Disclosure (57792):
    - Upgrade to Apache version 2.2.22 or later.

Remediation Plan for 172.26.21.112

You need to take the following 1 actions:

- Apache HTTP Server httpOnly Cookie Information Disclosure (57792):
    - Upgrade to Apache version 2.2.22 or later.

Remediation Plan for 172.26.22.1

You need to take the following 1 actions:

- HP Intelligent Management Center User Access Manager Unspecified Information Disclosure (65256):
    - Upgrade to HP Intelligent Management Center User Access Manager 5.2 E401 or later.

Remediation Plan for 172.26.22.15

You need to take the following 2 actions:

- Apache 2.2 < 2.2.24 Multiple Cross-Site Scripting Vulnerabilities (64912):
    - Either ensure that the affected modules are not in use or upgrade to Apache version 2.2.24 or later.
- HP Intelligent Management Center < 5.2 E401 Multiple Vulnerabilities (65255):
    - Upgrade to 5.2 E401 or later.

Remediation Plan for 172.26.22.23

You need to take the following 1 actions:

- MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check) (58435):
    - Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 : http://technet.microsoft.com/en-us/security/bulletin/ms12-020

Remediation Plan for 172.26.22.25

You need to take the following 2 actions:

- MS05-027: Vulnerability in SMB Could Allow Remote Code Execution (896422) (uncredentialed check) (18502):
    - Microsoft has released a set of patches for Windows 2000, XP and 2003 : http://technet.microsoft.com/en-us/security/bulletin/ms05-027
- MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check) (58435):
    - Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 : http://technet.microsoft.com/en-us/security/bulletin/ms12-020

Remediation Plan for 172.26.22.32

You need to take the following 1 actions:

- MySQL Default Account Credentials (61696):
    - Either remove the affected accounts or change the associated password.

Remediation Plan for 172.26.22.34

You need to take the following 1 actions:

- MySQL Default Account Credentials (61696):
    - Either remove the affected accounts or change the associated password.

Remediation Plan for 172.26.22.35

You need to take the following 1 actions:

- OpenSSL SSL*OP*NETSCAPE*REUSE*CIPHER*CHANGE*BUG Ciphersuite Disabled Cipher Issue (51893):
    - Upgrade to OpenSSL 0.9.8j or later.

Remediation Plan for 172.26.22.41

You need to take the following 2 actions:

- MS09-004: Vulnerability in Microsoft SQL Server Could Allow Remote Code Execution (959420) (uncredentialed check) (35635):
    - Microsoft has released a set of patches for SQL Server 2000 and 2005 : http://technet.microsoft.com/en-us/security/bulletin/ms09-004
- MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check) (58435):
    - Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 : http://technet.microsoft.com/en-us/security/bulletin/ms12-020

Remediation Plan for 172.26.22.46

You need to take the following 1 actions:

- VMware vCenter Server NFC Protocol Code Execution (VMSA-2013-0003) (65223):
    - Upgrade to VMware vCenter 4.0 update 4b, 5.0 before update 2, or 5.1 before 5.1.0b

Remediation Plan for 172.26.22.51

You need to take the following 1 actions:

- VMSA-2012-0009 : ESXi and ESX patches address critical security issues (uncredentialed check) (59447):
    - Apply the missing patches.

Remediation Plan for 172.26.22.55

You need to take the following 1 actions:

- VMware vCenter Server Denial of Service (VMSA-2012-0018) (65209):
  - Upgrade to VMware vCenter 4.1 Update 3 or 5.0 Update 2.

Remediation Plan for 172.26.22.60

You need to take the following 1 actions:

- Apache HTTP Server httpOnly Cookie Information Disclosure (57792):
  - Upgrade to Apache version 2.2.22 or later.

Remediation Plan for 172.26.22.67

You need to take the following 1 actions:

- Tomcat 4.1 XSS (47715):
  - Upgrade to Tomcat 4.1.29 or later.

Remediation Plan for 172.26.22.76

You need to take the following 1 actions:

- Tomcat 4.1 XSS (47715):
  - Upgrade to Tomcat 4.1.29 or later.

Remediation Plan for 172.26.22.82

You need to take the following 2 actions:

- MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check) (58435):
  - Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 : http://technet.microsoft.com/en-us/security/bulletin/ms12-020
- DB2 9.1 < Fix Pack 12 Multiple Vulnerabilities (60098):
  - Apply DB2 Version 9.1 Fix Pack 12 or later.

Remediation Plan for 172.26.22.100

You need to take the following 1 actions:

- Apache HTTP Server httpOnly Cookie Information Disclosure (57792):
  - Upgrade to Apache version 2.2.22 or later.

Remediation Plan for 172.26.22.104

You need to take the following 1 actions:

- DB2 10.1 < Fix Pack 1 Multiple Vulnerabilities (62369):
  - Apply DB2 Version 10.1 Fix Pack 1 or later.

Remediation Plan for 172.26.22.108

You need to take the following 1 actions:

- Oracle Database, January 2012 Critical Patch Update (57589):
  - Apply the January 2012 CPU.

Remediation Plan for 172.26.22.109

You need to take the following 1 actions:

- MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check) (58435):
  - Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 : http://technet.microsoft.com/en-us/security/bulletin/ms12-020

Remediation Plan for 172.26.22.113

You need to take the following 1 actions:

- HP LeftHand Virtual SAN Appliance < 10.0 hydra Service Multiple Remote Code Execution Vulnerabilities (version check) (64633):
    - Upgrade to HP LeftHand Virtual SAN Appliance version 10.0 or later.

Remediation Plan for 172.26.22.117

You need to take the following 1 actions:

- MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check) (58435):
    - Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 : http://technet.microsoft.com/en-us/security/bulletin/ms12-020

Remediation Plan for 172.26.22.134

You need to take the following 1 actions:

- MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check) (58435):
    - Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 : http://technet.microsoft.com/en-us/security/bulletin/ms12-020

Remediation Plan for 172.26.22.151

You need to take the following 1 actions:

- Apache Tomcat 6.0.x < 6.0.36 Multiple Vulnerabilities (62987):
    - Update Apache Tomcat to version 6.0.36 or later.

Remediation Plan for 172.26.22.156

You need to take the following 1 actions:

- MS09-004: Vulnerability in Microsoft SQL Server Could Allow Remote Code Execution (959420) (uncredentialed check) (35635):
    - Microsoft has released a set of patches for SQL Server 2000 and 2005 : http://technet.microsoft.com/en-us/security/bulletin/ms09-004

Remediation Plan for 172.26.22.195

You need to take the following 1 actions:

- Apache Tomcat 7.0.x < 7.0.32 CSRF Filter Bypass (63200):
    - Update Apache Tomcat to version 7.0.32 or later.

Remediation Plan for 172.26.22.211

You need to take the following 1 actions:

- Apache HTTP Server httpOnly Cookie Information Disclosure (57792):
    - Upgrade to Apache version 2.2.22 or later.

Remediation Plan for 172.26.22.212

You need to take the following 2 actions:

- Apache Tomcat 7.0.x < 7.0.32 CSRF Filter Bypass (63200):
    - Update Apache Tomcat to version 7.0.32 or later.
- VMware Security Updates for vCenter Server (VMSA-2013-0006) (66274):
    - Upgrade to VMware vCenter 5.1 update 1 or later.

Remediation Plan for 172.26.22.219

You need to take the following 1 actions:

- Apache HTTP Server httpOnly Cookie Information Disclosure (57792):
    - Upgrade to Apache version 2.2.22 or later.

Remediation Plan for 172.26.22.221

You need to take the following 1 actions:

- Apache HTTP Server httpOnly Cookie Information Disclosure (57792):
    - Upgrade to Apache version 2.2.22 or later.

Remediation Plan for 172.26.22.222

You need to take the following 1 actions:

- Tomcat 4.1 XSS (47715):
    - Upgrade to Tomcat 4.1.29 or later.

Remediation Plan for 172.26.22.240

You need to take the following 1 actions:

- Apache HTTP Server httpOnly Cookie Information Disclosure (57792):
    - Upgrade to Apache version 2.2.22 or later.

Remediation Plan for 172.26.22.241

You need to take the following 1 actions:

- MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check) (58435):
    - Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 : http://technet.microsoft.com/en-us/security/bulletin/ms12-020

Remediation Plan for 172.26.22.248

You need to take the following 1 actions:

- MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check) (58435):
    - Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 : http://technet.microsoft.com/en-us/security/bulletin/ms12-020

Remediation Plan for 172.26.22.249

You need to take the following 2 actions:

- MS05-027: Vulnerability in SMB Could Allow Remote Code Execution (896422) (uncredentialed check) (18502):
    - Microsoft has released a set of patches for Windows 2000, XP and 2003 : http://technet.microsoft.com/en-us/security/bulletin/ms05-027
- MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check) (58435):
    - Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 : http://technet.microsoft.com/en-us/security/bulletin/ms12-020

Remediation Plan for 172.26.22.250

You need to take the following 1 actions:

- MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check) (58435):
    - Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 : http://technet.microsoft.com/en-us/security/bulletin/ms12-020

Remediation Plan for 172.26.22.251

You need to take the following 1 actions:

- MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check) (58435):
    - Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 : http://technet.microsoft.com/en-us/security/bulletin/ms12-020

Remediation Plan for 172.26.22.252

You need to take the following 1 actions:

- MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check) (58435):
    - Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 : http://technet.microsoft.com/en-us/security/bulletin/ms12-020

Remediation Plan for 172.26.23.13

To patch the remote system, you need to install the following Microsoft patches:

- KB2808735 (MS13-036)
- KB2840149 (MS13-036)
- KB2813170 (MS13-031)
- KB2813347 (MS13-029)
- KB2817183 (MS13-028)
- KB2807986 (MS13-027)
- KB2814124 (MS13-022)
- KB2790113 (MS13-019)
- KB2790655 (MS13-018)
- KB2789642 (MS13-015)
- KB2789645 (MS13-015)
- KB2797052 (MS13-010)
- KB2736422 (MS13-007)
- KB2736428 (MS13-007)
- KB2785220 (MS13-006)
- KB2742595 (MS13-004)
- KB2742599 (MS13-004)
- KB2757638 (MS13-002)
- KB2769369 (MS13-001)
- KB2765809 (MS12-083)
- KB2770660 (MS12-082)
- KB2758857 (MS12-081)
- KB2753842 (MS12-078)
- KB2729449 (MS12-074)
- KB2729452 (MS12-074)
- KB2737019 (MS12-074)
- KB2719033 (MS12-073)
- KB2743555 (MS12-069)
- KB2565063 (MS11-025)

You need to take the following 2 actions:

- Adobe Reader < 11.0.2 / 10.1.6 / 9.5.4 Multiple Vulnerabilities (APSB13-07) (64786):
    - Upgrade to Adobe Reader 11.0.2 / 10.1.6 / 9.5.4 or later.
- Wireshark 1.8.x < 1.8.6 Multiple Vulnerabilities (65254):
    - Upgrade to Wireshark version 1.8.6 or later.

Remediation Plan for 172.26.23.18

To patch the remote system, you need to install the following Microsoft patches:

- KB2808735 (MS13-036)
- KB2840149 (MS13-036)
- KB2813170 (MS13-031)
- KB2817183 (MS13-028)
- KB2807986 (MS13-027)
- KB2814124 (MS13-022)
- KB2790113 (MS13-019)

- KB2790655 (MS13-018)
- KB2789642 (MS13-015)
- KB2789645 (MS13-015)
- KB2797052 (MS13-010)
- KB2736428 (MS13-007)
- KB2785220 (MS13-006)
- KB2742595 (MS13-004)
- KB2742599 (MS13-004)
- KB2757638 (MS13-002)
- KB2769369 (MS13-001)

Remediation Plan for 172.26.23.27

To patch the remote system, you need to install the following Microsoft patches:

- KB2808735 (MS13-036)
- KB2840149 (MS13-036)
- KB2813170 (MS13-031)
- KB2813347 (MS13-029)
- KB2817183 (MS13-028)
- KB2807986 (MS13-027)
- KB2814124 (MS13-022)
- KB2790113 (MS13-019)
- KB2790655 (MS13-018)
- KB2789642 (MS13-015)
- KB2789645 (MS13-015)
- KB2797052 (MS13-010)
- KB2736428 (MS13-007)
- KB2785220 (MS13-006)
- KB2742595 (MS13-004)
- KB2742599 (MS13-004)
- KB2757638 (MS13-002)
- KB2769369 (MS13-001)
- KB2765809 (MS12-083)
- KB2770660 (MS12-082)
- KB2758857 (MS12-081)
- KB2753842 (MS12-078)
- KB2729449 (MS12-074)
- KB2729452 (MS12-074)
- KB2737019 (MS12-074)
- KB2743555 (MS12-069)

Remediation Plan for 172.26.23.33

To patch the remote system, you need to install the following Microsoft patches:

- KB2808735 (MS13-036)
- KB2840149 (MS13-036)
- KB2813170 (MS13-031)
- KB2813347 (MS13-029)
- KB2817183 (MS13-028)
- KB2807986 (MS13-027)
- KB2814124 (MS13-022)
- KB2790113 (MS13-019)
- KB2790655 (MS13-018)
- KB2789642 (MS13-015)
- KB2789645 (MS13-015)
- KB2797052 (MS13-010)
- KB2736422 (MS13-007)
- KB2736428 (MS13-007)
- KB2785220 (MS13-006)
- KB2742595 (MS13-004)
- KB2742599 (MS13-004)
- KB2757638 (MS13-002)
- KB2769369 (MS13-001)
- KB2765809 (MS12-083)
- KB2770660 (MS12-082)
- KB2758857 (MS12-081)

- KB2753842 (MS12-078)
- KB2729449 (MS12-074)
- KB2729452 (MS12-074)
- KB2737019 (MS12-074)
- KB2743555 (MS12-069)

Remediation Plan for 172.26.23.41

To patch the remote system, you need to install the following Microsoft patches:

- KB2808735 (MS13-036)
- KB2840149 (MS13-036)
- KB2813170 (MS13-031)
- KB2813347 (MS13-029)
- KB2817183 (MS13-028)
- KB2807986 (MS13-027)
- KB2814124 (MS13-022)
- KB2790113 (MS13-019)
- KB2790655 (MS13-018)
- KB2789642 (MS13-015)
- KB2789645 (MS13-015)
- KB2797052 (MS13-010)
- KB2736428 (MS13-007)
- KB2785220 (MS13-006)
- KB2742595 (MS13-004)
- KB2742599 (MS13-004)
- (MS13-002)
- KB2757638 (MS13-002)
- KB2769369 (MS13-001)
- KB2765809 (MS12-083)
- KB2770660 (MS12-082)
- KB2758857 (MS12-081)
- KB2753842 (MS12-078)
- KB2687311 (MS12-076)
- KB2729449 (MS12-074)
- KB2729452 (MS12-074)
- KB2737019 (MS12-074)
- KB2743555 (MS12-069)
- KB2687439 (MS12-066)
- KB2687440 (MS12-066)
- KB2687441 (MS12-060)
- (MS12-043)
- KB2596912 (MS11-094)
- KB2596705 (MS11-091)
- KB2552997 (MS11-074)
- KB2289078 (MS10-105)
- KB979441 (MS10-039)
- KB973709 (MS09-060)
- KB950130 (MS08-055)
- KB946983 (MS08-015)

You need to take the following 1 actions:

- Flash Player <= 10.3.183.68 / 11.6.602.180 Multiple Vulnerabilities (APSB13-11) (65910):
  - Upgrade to Adobe Flash Player version 10.3.183.75 / 11.7.700.169 or later, or Google Chrome PepperFlash 11.7.700.179 or later.

Remediation Plan for 172.26.23.43

To patch the remote system, you need to install the following Microsoft patches:

- KB2808735 (MS13-036)
- KB2840149 (MS13-036)
- KB2813170 (MS13-031)
- KB2813347 (MS13-029)
- KB2817183 (MS13-028)
- KB2807986 (MS13-027)
- KB2814124 (MS13-022)

- KB2790113 (MS13-019)
- KB2790655 (MS13-018)
- KB2789642 (MS13-015)
- KB2789645 (MS13-015)
- KB2797052 (MS13-010)
- KB2736428 (MS13-007)
- KB2785220 (MS13-006)
- KB2742595 (MS13-004)
- KB2742599 (MS13-004)
- KB2757638 (MS13-002)
- KB2769369 (MS13-001)
- KB2765809 (MS12-083)
- KB2770660 (MS12-082)
- KB2758857 (MS12-081)
- KB2753842 (MS12-078)
- KB2729449 (MS12-074)
- KB2729452 (MS12-074)
- KB2737019 (MS12-074)
- KB2743555 (MS12-069)

You need to take the following 1 actions:

- Flash Player <= 10.3.183.68 / 11.6.602.180 Multiple Vulnerabilities (APSB13-11) (65910):
  - Upgrade to Adobe Flash Player version 10.3.183.75 / 11.7.700.169 or later, or Google Chrome PepperFlash 11.7.700.179 or later.

Remediation Plan for 172.26.23.62

To patch the remote system, you need to install the following Microsoft patches:

- KB2808735 (MS13-036)
- KB2840149 (MS13-036)
- KB2813170 (MS13-031)
- KB2813347 (MS13-029)
- KB2817183 (MS13-028)
- KB2807986 (MS13-027)
- KB2814124 (MS13-022)
- KB2790113 (MS13-019)
- KB2790655 (MS13-018)
- KB2789642 (MS13-015)
- KB2789645 (MS13-015)
- KB2797052 (MS13-010)

Remediation Plan for 172.26.23.73

To patch the remote system, you need to install the following Microsoft patches:

- KB2808735 (MS13-036)
- KB2840149 (MS13-036)
- KB2813170 (MS13-031)
- KB2813347 (MS13-029)
- KB2817183 (MS13-028)
- KB2807986 (MS13-027)
- KB2814124 (MS13-022)
- KB2790113 (MS13-019)
- KB2790655 (MS13-018)
- KB2789642 (MS13-015)
- KB2789645 (MS13-015)
- KB2797052 (MS13-010)
- KB2736428 (MS13-007)
- KB2785220 (MS13-006)
- KB2742595 (MS13-004)
- KB2742599 (MS13-004)
- KB2757638 (MS13-002)
- KB2769369 (MS13-001)
- KB2765809 (MS12-083)
- KB2770660 (MS12-082)
- KB2758857 (MS12-081)

- KB2753842 (MS12-078)
- KB2729449 (MS12-074)
- KB2729452 (MS12-074)
- KB2737019 (MS12-074)
- KB2743555 (MS12-069)

Remediation Plan for 172.26.23.83

You need to take the following 1 actions:

- MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check) (58435):
  - Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 : http://technet.microsoft.com/en-us/security/bulletin/ms12-020

Remediation Plan for 172.26.23.105

You need to take the following 1 actions:

- Multiple Mail Server EXPN/VRFY Information Disclosure (10249):
  - If you are using Sendmail, add the option : O PrivacyOptions=goaway in /etc/sendmail.cf.

Remediation Plan for 172.26.23.107

You need to take the following 1 actions:

- SAP MaxDB Multiple Vulnerabilities (32194):
  - Upgrade to SAP MaxDB 7.7.04 Build 08 / 7.7.03 Build 23 / 7.7.02 Build 20 / 7.6.05 Build 02 / 7.6.04 Build 06 / 7.6.03 Build 15 / 7.5.00 Build 48 or later.

Remediation Plan for 172.26.23.112

You need to take the following 1 actions:

- Apache HTTP Server httpOnly Cookie Information Disclosure (57792):
  - Upgrade to Apache version 2.2.22 or later.

Remediation Plan for 172.26.23.117

You need to take the following 1 actions:

- SAP MaxDB Multiple Vulnerabilities (32194):
  - Upgrade to SAP MaxDB 7.7.04 Build 08 / 7.7.03 Build 23 / 7.7.02 Build 20 / 7.6.05 Build 02 / 7.6.04 Build 06 / 7.6.03 Build 15 / 7.5.00 Build 48 or later.

Remediation Plan for 172.26.23.128

You need to take the following 1 actions:

- SAP MaxDB Multiple Vulnerabilities (32194):
  - Upgrade to SAP MaxDB 7.7.04 Build 08 / 7.7.03 Build 23 / 7.7.02 Build 20 / 7.6.05 Build 02 / 7.6.04 Build 06 / 7.6.03 Build 15 / 7.5.00 Build 48 or later.

Remediation Plan for 172.26.23.131

You need to take the following 1 actions:

- Apache HTTP Server httpOnly Cookie Information Disclosure (57792):
  - Upgrade to Apache version 2.2.22 or later.

Remediation Plan for 172.26.23.138

You need to take the following 1 actions:

- HP LeftHand Virtual SAN Appliance < 10.0 hydra Service Multiple Remote Code Execution Vulnerabilities (version check) (64633):
  - Upgrade to HP LeftHand Virtual SAN Appliance version 10.0 or later.

Remediation Plan for 172.26.23.145

To patch the remote system, you need to install the following Microsoft patches:

- KB2808735 (MS13-036)
- KB2840149 (MS13-036)
- KB2813170 (MS13-031)
- KB2813347 (MS13-029)
- KB2817183 (MS13-028)
- KB2807986 (MS13-027)
- KB2814124 (MS13-022)
- KB2790113 (MS13-019)
- KB2790655 (MS13-018)
- KB2789642 (MS13-015)
- KB2789645 (MS13-015)
- KB2797052 (MS13-010)
- KB2736428 (MS13-007)
- KB2785220 (MS13-006)
- KB2742595 (MS13-004)
- KB2742599 (MS13-004)
- KB2757638 (MS13-002)
- KB2769369 (MS13-001)
- KB2765809 (MS12-083)
- KB2770660 (MS12-082)
- KB2758857 (MS12-081)
- KB2753842 (MS12-078)
- KB2729449 (MS12-074)
- KB2729452 (MS12-074)
- KB2737019 (MS12-074)
- KB2743555 (MS12-069)

Remediation Plan for 172.26.23.157

You need to take the following 1 actions:

- SAP MaxDB Multiple Vulnerabilities (32194):
  - Upgrade to SAP MaxDB 7.7.04 Build 08 / 7.7.03 Build 23 / 7.7.02 Build 20 / 7.6.05 Build 02 / 7.6.04 Build 06 / 7.6.03 Build 15 / 7.5.00 Build 48 or later.

Remediation Plan for 172.26.23.158

You need to take the following 2 actions:

- DB2 9.7 < Fix Pack 7 Multiple Vulnerabilities (62701):
  - Apply DB2 Version 9.7 Fix Pack 7 or later.
- IBM WebSphere Application Server 8.0 < Fix Pack 6 Multiple Vulnerabilities (66374):
  - Apply Fix Pack 6 for version 8.0 (8.0.0.6) or later.

Remediation Plan for 172.26.23.165

You need to take the following 1 actions:

- HP LeftHand Virtual SAN Appliance < 10.0 hydra Service Multiple Remote Code Execution Vulnerabilities (version check) (64633):
  - Upgrade to HP LeftHand Virtual SAN Appliance version 10.0 or later.

Remediation Plan for 172.26.23.170

You need to take the following 1 actions:

- SAP MaxDB Multiple Vulnerabilities (32194):
  - Upgrade to SAP MaxDB 7.7.04 Build 08 / 7.7.03 Build 23 / 7.7.02 Build 20 / 7.6.05 Build 02 / 7.6.04 Build 06 / 7.6.03 Build 15 / 7.5.00 Build 48 or later.

Remediation Plan for 172.26.23.173

You need to take the following 1 actions:

- Apache HTTP Server httpOnly Cookie Information Disclosure (57792):
    - Upgrade to Apache version 2.2.22 or later.

Remediation Plan for 172.26.23.182

You need to take the following 1 actions:

- Apache HTTP Server httpOnly Cookie Information Disclosure (57792):
    - Upgrade to Apache version 2.2.22 or later.

Remediation Plan for 172.26.23.186

You need to take the following 1 actions:

- MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check) (58435):
    - Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 : http://technet.microsoft.com/en-us/security/bulletin/ms12-020

Remediation Plan for 172.26.23.188

You need to take the following 1 actions:

- Apache HTTP Server httpOnly Cookie Information Disclosure (57792):
    - Upgrade to Apache version 2.2.22 or later.

Remediation Plan for 172.26.32.135

You need to take the following 2 actions:

- Apache Tomcat 6.0.x < 6.0.36 Multiple Vulnerabilities (62987):
    - Update Apache Tomcat to version 6.0.36 or later.
- McAfee ePolicy Orchestrator 4.6.x Multiple Vulnerabilities (SB10042) (66319):
    - Upgrade to ePolicy Orchestrator 4.6.6 / 5.0 or later.

Remediation Plan for 172.26.32.214

You need to take the following 1 actions:

- Apache HTTP Server httpOnly Cookie Information Disclosure (57792):
    - Upgrade to Apache version 2.2.22 or later.

Remediation Plan for 172.26.33.234

You need to take the following 1 actions:

- Apache 2.2 < 2.2.24 Multiple Cross-Site Scripting Vulnerabilities (64912):
    - Either ensure that the affected modules are not in use or upgrade to Apache version 2.2.24 or later.

Remediation Plan for 172.26.34.30

You need to take the following 1 actions:

- Apache Tomcat < 4.1.40 / 5.5.28 / 6.0.20 Multiple Vulnerabilities (46753):
    - Update Apache Tomcat to version 4.1.40 / 5.5.28 / 6.0.20 or later.

Remediation Plan for 172.26.34.184

You need to take the following 1 actions:

- Web Server HTTP Header Internal IP Disclosure (10759):
    - None

Remediation Plan for 172.26.48.26

You need to take the following 1 actions:

- Apache HTTP Server httpOnly Cookie Information Disclosure (57792):
    - Upgrade to Apache version 2.2.22 or later.

Remediation Plan for 172.26.48.28

You need to take the following 1 actions:

- Portable OpenSSH ssh-keysign ssh-rand-helper Utility File Descriptor Leak Local Information Disclosure (53841):
    - Upgrade to Portable OpenSSH 5.8p2 or later.

Remediation Plan for 172.26.48.31

You need to take the following 1 actions:

- Portable OpenSSH ssh-keysign ssh-rand-helper Utility File Descriptor Leak Local Information Disclosure (53841):
    - Upgrade to Portable OpenSSH 5.8p2 or later.

Remediation Plan for 172.26.48.45

You need to take the following 27 actions:

- RHEL 2.1 / 3 / 4 / 5 : e2fsprogs (RHSA-2008-0003) (29876):
    - Update the affected e2fsprogs, e2fsprogs-devel and / or e2fsprogs-libs packages.
- RHEL 2.1 / 3 : unzip (RHSA-2008-0196) (31619):
    - Update the affected unzip package.
- RHEL 3 : XFree86 (RHSA-2008-0502) (33151):
    - Update the affected packages.
- RHEL 3 / 4 / 5 : ipsec-tools (RHSA-2008-0849) (34054):
    - Update the affected ipsec-tools package.
- RHEL 2.1 / 3 / 4 / 5 : ed (RHSA-2008-0946) (34467):
    - Update the affected ed package.
- RHEL 3 / 4 : vim (RHSA-2008-0617) (34954):
    - Update the affected packages.
- RHEL 3 : net-snmp (RHSA-2009-1124) (39527):
    - Update the affected packages.
- RHEL 3 : python (RHSA-2009-1178) (40402):
    - Update the affected packages.
- RHEL 3 : bind (RHSA-2009-1181) (40433):
    - Update the affected packages.
- RHEL 3 / 4 / 5 : libxml and libxml2 (RHSA-2009-1206) (40544):
    - Update the affected packages.
- RHEL 3 / 4 / 5 : newt (RHSA-2009-1463) (41620):
    - Update the affected newt and / or newt-devel packages.
- RHEL 3 / 4 / 5 : wget (RHSA-2009-1549) (42359):
    - Update the affected wget package.
- RHEL 3 : kernel (RHSA-2009-1550) (42360):
    - Update the affected packages.
- RHEL 3 / 4 / 5 : expat (RHSA-2009-1625) (43046):
    - Update the affected expat and / or expat-devel packages.
- RHEL 3 / 4 / 5 : libtool (RHSA-2009-1646) (43078):
    - Update the affected packages.
- RHEL 3 / 4 / 5 : gcc and gcc4 (RHSA-2010-0039) (43882):
    - Update the affected packages.
- RHEL 3 / 4 / 5 : gzip (RHSA-2010-0061) (44104):
    - Update the affected gzip package.
- RHEL 3 : tar (RHSA-2010-0142) (46265):
    - Update the affected tar package.
- RHEL 3 : cpio (RHSA-2010-0145) (46268):
    - Update the affected cpio package.
- RHEL 3 / 4 : openssl (RHSA-2010-0163) (46274):
    - Update the affected openssl, openssl-devel and / or openssl-perl packages.
- RHEL 3 / 4 / 5 : krb5 (RHSA-2010-0423) (46665):
    - Update the affected packages.
- RHEL 3 / 4 : perl (RHSA-2010-0457) (46833):
    - Update the affected packages.
- RHEL 3 : libtiff (RHSA-2010-0520) (47873):
    - Update the affected libtiff and / or libtiff-devel packages.
- RHEL 3 / 4 / 5 : libpng (RHSA-2010-0534) (47876):

    - Update the affected packages.
- RHEL 3 / 4 / 5 : bzip2 (RHSA-2010-0703) (49301):
    - Update the affected bzip2, bzip2-devel and / or bzip2-libs packages.
- RHEL 3 : freetype (RHSA-2010-0736) (49748):
    - Update the affected freetype and / or freetype-devel packages.
- RHEL 3 : cups (RHSA-2010-0754) (49801):
    - Update the affected cups, cups-devel and / or cups-libs packages.

Remediation Plan for 172.26.48.46

You need to take the following 42 actions:

- RHEL 2.1 / 3 / 4 / 5 : e2fsprogs (RHSA-2008-0003) (29876):
    - Update the affected e2fsprogs, e2fsprogs-devel and / or e2fsprogs-libs packages.
- RHEL 4 : tk (RHSA-2008-0135) (31161):
    - Update the affected tk and / or tk-devel packages.
- RHEL 4 / 5 : bluez-libs and bluez-utils (RHSA-2008-0581) (33497):
    - Update the affected packages.
- RHEL 4 : coreutils (RHSA-2008-0780) (33586):
    - Update the affected coreutils package.
- RHEL 4 / 5 : libxslt (RHSA-2008-0649) (33784):
    - Update the affected libxslt, libxslt-devel and / or libxslt-python packages.
- RHEL 4 / 5 : openssh (RHSA-2008-0855) (34034):
    - Update the affected packages.
- RHEL 3 / 4 / 5 : ipsec-tools (RHSA-2008-0849) (34054):
    - Update the affected ipsec-tools package.
- RHEL 2.1 / 3 / 4 / 5 : ed (RHSA-2008-0946) (34467):
    - Update the affected ed package.
- RHEL 3 / 4 / 5 : net-snmp (RHSA-2008-0971) (34691):
    - Update the affected packages.
- RHEL 3 / 4 : vim (RHSA-2008-0617) (34954):
    - Update the affected packages.
- RHEL 4 : NetworkManager (RHSA-2009-0362) (36031):
    - Update the affected NetworkManager and / or NetworkManager-gnome packages.
- RHEL 3 / 4 / 5 : acpid (RHSA-2009-0474) (38710):
    - Update the affected acpid package.
- RHEL 4 : nfs-utils (RHSA-2009-0955) (38816):
    - Update the affected nfs-utils package.
- RHEL 4 : util-linux (RHSA-2009-0981) (38817):
    - Update the affected util-linux package.
- RHEL 3 / 4 / 5 : newt (RHSA-2009-1463) (41620):
    - Update the affected newt and / or newt-devel packages.
- RHEL 3 / 4 / 5 : wget (RHSA-2009-1549) (42359):
    - Update the affected wget package.
- RHEL 3 / 4 / 5 : expat (RHSA-2009-1625) (43046):
    - Update the affected expat and / or expat-devel packages.
- RHEL 3 / 4 / 5 : gcc and gcc4 (RHSA-2010-0039) (43882):
    - Update the affected packages.
- RHEL 3 / 4 / 5 : gzip (RHSA-2010-0061) (44104):
    - Update the affected gzip package.
- RHEL 4 / 5 : tar (RHSA-2010-0141) (46264):
    - Update the affected tar package.
- RHEL 4 : cpio (RHSA-2010-0143) (46266):
    - Update the affected cpio package.
- RHEL 4 : openldap (RHSA-2010-0543) (47878):
    - Update the affected packages.
- RHEL 3 / 4 / 5 : bzip2 (RHSA-2010-0703) (49301):
    - Update the affected bzip2, bzip2-devel and / or bzip2-libs packages.
- RHEL 4 : cups (RHSA-2010-0755) (49802):
    - Update the affected cups, cups-devel and / or cups-libs packages.
- RHEL 4 / 5 / 6 : libuser (RHSA-2011-0170) (51590):
    - Update the affected packages.
- RHEL 4 : bash (RHSA-2011-0261) (52008):
    - Update the affected bash package.
- RHEL 4 : kernel (RHSA-2011-0263) (52009):
    - Update the affected packages.
- RHEL 4 / 5 / 6 : libtiff (RHSA-2011-0392) (53206):
    - Update the affected packages.

- RHEL 4 : sendmail (RHSA-2011-0262) (53535):
  - Update the affected packages.
- RHEL 4 / 5 : xmlsec1 (RHSA-2011-0486) (53646):
  - Update the affected packages.
- RHEL 4 : python (RHSA-2011-0491) (53820):
  - Update the affected packages.
- RHEL 4 / 5 / 6 : dhcp (RHSA-2011-1160) (55855):
  - Update the affected packages.
- RHEL 4 / 5 / 6 : rpm (RHSA-2011-1349) (56383):
  - Update the affected packages.
- RHEL 4 : xorg-x11 (RHSA-2011-1360) (56411):
  - Update the affected packages.
- RHEL 4 / 5 / 6 : freetype (RHSA-2011-1455) (56859):
  - Update the affected packages.
- RHEL 4 : bind (RHSA-2011-1496) (56975):
  - Update the affected packages.
- RHEL 4 / 5 : perl (RHSA-2011-1797) (57053):
  - Update the affected perl and / or perl-suidperl packages.
- RHEL 4 / 5 : krb5 (RHSA-2011-1851) (57408):
  - Update the affected packages.
- RHEL 4 : libxml2 (RHSA-2012-0016) (57491):
  - Update the affected libxml2, libxml2-devel and / or libxml2-python packages.
- RHEL 4 : openssl (RHSA-2012-0086) (57789):
  - Update the affected openssl, openssl-devel and / or openssl-perl packages.
- RHEL 4 : glibc (RHSA-2012-0125) (57928):
  - Update the affected packages.
- RHEL 4 / 5 / 6 : libpng (RHSA-2012-0317) (58068):
  - Update the affected packages.

Remediation Plan for 172.26.48.47

You need to take the following 41 actions:

- RHEL 4 : tk (RHSA-2008-0135) (31161):
  - Update the affected tk and / or tk-devel packages.
- RHEL 4 / 5 : bluez-libs and bluez-utils (RHSA-2008-0581) (33497):
  - Update the affected packages.
- RHEL 4 : coreutils (RHSA-2008-0780) (33586):
  - Update the affected coreutils package.
- RHEL 4 / 5 : libxslt (RHSA-2008-0649) (33784):
  - Update the affected libxslt, libxslt-devel and / or libxslt-python packages.
- RHEL 4 / 5 : openssh (RHSA-2008-0855) (34034):
  - Update the affected packages.
- RHEL 3 / 4 / 5 : ipsec-tools (RHSA-2008-0849) (34054):
  - Update the affected ipsec-tools package.
- RHEL 2.1 / 3 / 4 / 5 : ed (RHSA-2008-0946) (34467):
  - Update the affected ed package.
- RHEL 3 / 4 / 5 : net-snmp (RHSA-2008-0971) (34691):
  - Update the affected packages.
- RHEL 3 / 4 : vim (RHSA-2008-0617) (34954):
  - Update the affected packages.
- RHEL 4 : NetworkManager (RHSA-2009-0362) (36031):
  - Update the affected NetworkManager and / or NetworkManager-gnome packages.
- RHEL 3 / 4 / 5 : acpid (RHSA-2009-0474) (38710):
  - Update the affected acpid package.
- RHEL 4 : nfs-utils (RHSA-2009-0955) (38816):
  - Update the affected nfs-utils package.
- RHEL 4 : util-linux (RHSA-2009-0981) (38817):
  - Update the affected util-linux package.
- RHEL 3 / 4 / 5 : newt (RHSA-2009-1463) (41620):
  - Update the affected newt and / or newt-devel packages.
- RHEL 3 / 4 / 5 : wget (RHSA-2009-1549) (42359):
  - Update the affected wget package.
- RHEL 3 / 4 / 5 : expat (RHSA-2009-1625) (43046):
  - Update the affected expat and / or expat-devel packages.
- RHEL 3 / 4 / 5 : gcc and gcc4 (RHSA-2010-0039) (43882):
  - Update the affected packages.
- RHEL 3 / 4 / 5 : gzip (RHSA-2010-0061) (44104):

    - Update the affected gzip package.
- RHEL 4 / 5 : tar (RHSA-2010-0141) (46264):
    - Update the affected tar package.
- RHEL 4 : cpio (RHSA-2010-0143) (46266):
    - Update the affected cpio package.
- RHEL 4 : openldap (RHSA-2010-0543) (47878):
    - Update the affected packages.
- RHEL 3 / 4 / 5 : bzip2 (RHSA-2010-0703) (49301):
    - Update the affected bzip2, bzip2-devel and / or bzip2-libs packages.
- RHEL 4 : cups (RHSA-2010-0755) (49802):
    - Update the affected cups, cups-devel and / or cups-libs packages.
- RHEL 4 / 5 / 6 : libuser (RHSA-2011-0170) (51590):
    - Update the affected packages.
- RHEL 4 : bash (RHSA-2011-0261) (52008):
    - Update the affected bash package.
- RHEL 4 : kernel (RHSA-2011-0263) (52009):
    - Update the affected packages.
- RHEL 4 / 5 / 6 : libtiff (RHSA-2011-0392) (53206):
    - Update the affected packages.
- RHEL 4 : sendmail (RHSA-2011-0262) (53535):
    - Update the affected packages.
- RHEL 4 / 5 : xmlsec1 (RHSA-2011-0486) (53646):
    - Update the affected packages.
- RHEL 4 : python (RHSA-2011-0491) (53820):
    - Update the affected packages.
- RHEL 4 / 5 / 6 : dhcp (RHSA-2011-1160) (55855):
    - Update the affected packages.
- RHEL 4 / 5 / 6 : rpm (RHSA-2011-1349) (56383):
    - Update the affected packages.
- RHEL 4 : xorg-x11 (RHSA-2011-1360) (56411):
    - Update the affected packages.
- RHEL 4 / 5 / 6 : freetype (RHSA-2011-1455) (56859):
    - Update the affected packages.
- RHEL 4 : bind (RHSA-2011-1496) (56975):
    - Update the affected packages.
- RHEL 4 / 5 : perl (RHSA-2011-1797) (57053):
    - Update the affected perl and / or perl-suidperl packages.
- RHEL 4 / 5 : krb5 (RHSA-2011-1851) (57408):
    - Update the affected packages.
- RHEL 4 : libxml2 (RHSA-2012-0016) (57491):
    - Update the affected libxml2, libxml2-devel and / or libxml2-python packages.
- RHEL 4 : openssl (RHSA-2012-0086) (57789):
    - Update the affected openssl, openssl-devel and / or openssl-perl packages.
- RHEL 4 : glibc (RHSA-2012-0125) (57928):
    - Update the affected packages.
- RHEL 4 / 5 / 6 : libpng (RHSA-2012-0317) (58068):
    - Update the affected packages.

Remediation Plan for 172.26.48.48

You need to take the following 41 actions:

- RHEL 4 : tk (RHSA-2008-0135) (31161):
    - Update the affected tk and / or tk-devel packages.
- RHEL 4 / 5 : bluez-libs and bluez-utils (RHSA-2008-0581) (33497):
    - Update the affected packages.
- RHEL 4 : coreutils (RHSA-2008-0780) (33586):
    - Update the affected coreutils package.
- RHEL 4 / 5 : libxslt (RHSA-2008-0649) (33784):
    - Update the affected libxslt, libxslt-devel and / or libxslt-python packages.
- RHEL 4 / 5 : openssh (RHSA-2008-0855) (34034):
    - Update the affected packages.
- RHEL 3 / 4 / 5 : ipsec-tools (RHSA-2008-0849) (34054):
    - Update the affected ipsec-tools package.
- RHEL 2.1 / 3 / 4 / 5 : ed (RHSA-2008-0946) (34467):
    - Update the affected ed package.
- RHEL 3 / 4 / 5 : net-snmp (RHSA-2008-0971) (34691):
    - Update the affected packages.

- RHEL 3 / 4 : vim (RHSA-2008-0617) (34954):
  - Update the affected packages.
- RHEL 4 : NetworkManager (RHSA-2009-0362) (36031):
  - Update the affected NetworkManager and / or NetworkManager-gnome packages.
- RHEL 3 / 4 / 5 : acpid (RHSA-2009-0474) (38710):
  - Update the affected acpid package.
- RHEL 4 : nfs-utils (RHSA-2009-0955) (38816):
  - Update the affected nfs-utils package.
- RHEL 4 : util-linux (RHSA-2009-0981) (38817):
  - Update the affected util-linux package.
- RHEL 3 / 4 / 5 : newt (RHSA-2009-1463) (41620):
  - Update the affected newt and / or newt-devel packages.
- RHEL 3 / 4 / 5 : wget (RHSA-2009-1549) (42359):
  - Update the affected wget package.
- RHEL 3 / 4 / 5 : expat (RHSA-2009-1625) (43046):
  - Update the affected expat and / or expat-devel packages.
- RHEL 3 / 4 / 5 : gcc and gcc4 (RHSA-2010-0039) (43882):
  - Update the affected packages.
- RHEL 3 / 4 / 5 : gzip (RHSA-2010-0061) (44104):
  - Update the affected gzip package.
- RHEL 4 / 5 : tar (RHSA-2010-0141) (46264):
  - Update the affected tar package.
- RHEL 4 : cpio (RHSA-2010-0143) (46266):
  - Update the affected cpio package.
- RHEL 4 : openldap (RHSA-2010-0543) (47878):
  - Update the affected packages.
- RHEL 3 / 4 / 5 : bzip2 (RHSA-2010-0703) (49301):
  - Update the affected bzip2, bzip2-devel and / or bzip2-libs packages.
- RHEL 4 : cups (RHSA-2010-0755) (49802):
  - Update the affected cups, cups-devel and / or cups-libs packages.
- RHEL 4 / 5 / 6 : libuser (RHSA-2011-0170) (51590):
  - Update the affected packages.
- RHEL 4 : bash (RHSA-2011-0261) (52008):
  - Update the affected bash package.
- RHEL 4 : kernel (RHSA-2011-0263) (52009):
  - Update the affected packages.
- RHEL 4 / 5 / 6 : libtiff (RHSA-2011-0392) (53206):
  - Update the affected packages.
- RHEL 4 : sendmail (RHSA-2011-0262) (53535):
  - Update the affected packages.
- RHEL 4 / 5 : xmlsec1 (RHSA-2011-0486) (53646):
  - Update the affected packages.
- RHEL 4 : python (RHSA-2011-0491) (53820):
  - Update the affected packages.
- RHEL 4 / 5 / 6 : dhcp (RHSA-2011-1160) (55855):
  - Update the affected packages.
- RHEL 4 / 5 / 6 : rpm (RHSA-2011-1349) (56383):
  - Update the affected packages.
- RHEL 4 : xorg-x11 (RHSA-2011-1360) (56411):
  - Update the affected packages.
- RHEL 4 / 5 / 6 : freetype (RHSA-2011-1455) (56859):
  - Update the affected packages.
- RHEL 4 : bind (RHSA-2011-1496) (56975):
  - Update the affected packages.
- RHEL 4 / 5 : perl (RHSA-2011-1797) (57053):
  - Update the affected perl and / or perl-suidperl packages.
- RHEL 4 / 5 : krb5 (RHSA-2011-1851) (57408):
  - Update the affected packages.
- RHEL 4 : libxml2 (RHSA-2012-0016) (57491):
  - Update the affected libxml2, libxml2-devel and / or libxml2-python packages.
- RHEL 4 : openssl (RHSA-2012-0086) (57789):
  - Update the affected openssl, openssl-devel and / or openssl-perl packages.
- RHEL 4 : glibc (RHSA-2012-0125) (57928):
  - Update the affected packages.
- RHEL 4 / 5 / 6 : libpng (RHSA-2012-0317) (58068):
  - Update the affected packages.

Remediation Plan for 172.26.48.49

You need to take the following 40 actions:

- RHEL 4 : tk (RHSA-2008-0135) (31161):
  - Update the affected tk and / or tk-devel packages.
- RHEL 4 / 5 : bluez-libs and bluez-utils (RHSA-2008-0581) (33497):
  - Update the affected packages.
- RHEL 4 : coreutils (RHSA-2008-0780) (33586):
  - Update the affected coreutils package.
- RHEL 4 / 5 : libxslt (RHSA-2008-0649) (33784):
  - Update the affected libxslt, libxslt-devel and / or libxslt-python packages.
- RHEL 4 / 5 : openssh (RHSA-2008-0855) (34034):
  - Update the affected packages.
- RHEL 3 / 4 / 5 : ipsec-tools (RHSA-2008-0849) (34054):
  - Update the affected ipsec-tools package.
- RHEL 2.1 / 3 / 4 / 5 : ed (RHSA-2008-0946) (34467):
  - Update the affected ed package.
- RHEL 3 / 4 / 5 : net-snmp (RHSA-2008-0971) (34691):
  - Update the affected packages.
- RHEL 3 / 4 : vim (RHSA-2008-0617) (34954):
  - Update the affected packages.
- RHEL 4 : NetworkManager (RHSA-2009-0362) (36031):
  - Update the affected NetworkManager and / or NetworkManager-gnome packages.
- RHEL 3 / 4 / 5 : acpid (RHSA-2009-0474) (38710):
  - Update the affected acpid package.
- RHEL 4 : nfs-utils (RHSA-2009-0955) (38816):
  - Update the affected nfs-utils package.
- RHEL 4 : util-linux (RHSA-2009-0981) (38817):
  - Update the affected util-linux package.
- RHEL 3 / 4 / 5 : newt (RHSA-2009-1463) (41620):
  - Update the affected newt and / or newt-devel packages.
- RHEL 3 / 4 / 5 : wget (RHSA-2009-1549) (42359):
  - Update the affected wget package.
- RHEL 3 / 4 / 5 : expat (RHSA-2009-1625) (43046):
  - Update the affected expat and / or expat-devel packages.
- RHEL 3 / 4 / 5 : gcc and gcc4 (RHSA-2010-0039) (43882):
  - Update the affected packages.
- RHEL 4 / 5 : tar (RHSA-2010-0141) (46264):
  - Update the affected tar package.
- RHEL 4 : cpio (RHSA-2010-0143) (46266):
  - Update the affected cpio package.
- RHEL 4 : openldap (RHSA-2010-0543) (47878):
  - Update the affected packages.
- RHEL 3 / 4 / 5 : bzip2 (RHSA-2010-0703) (49301):
  - Update the affected bzip2, bzip2-devel and / or bzip2-libs packages.
- RHEL 4 : cups (RHSA-2010-0755) (49802):
  - Update the affected cups, cups-devel and / or cups-libs packages.
- RHEL 4 / 5 / 6 : libuser (RHSA-2011-0170) (51590):
  - Update the affected packages.
- RHEL 4 : bash (RHSA-2011-0261) (52008):
  - Update the affected bash package.
- RHEL 4 : kernel (RHSA-2011-0263) (52009):
  - Update the affected packages.
- RHEL 4 / 5 / 6 : libtiff (RHSA-2011-0392) (53206):
  - Update the affected packages.
- RHEL 4 : sendmail (RHSA-2011-0262) (53535):
  - Update the affected packages.
- RHEL 4 / 5 : xmlsec1 (RHSA-2011-0486) (53646):
  - Update the affected packages.
- RHEL 4 : python (RHSA-2011-0491) (53820):
  - Update the affected packages.
- RHEL 4 / 5 / 6 : dhcp (RHSA-2011-1160) (55855):
  - Update the affected packages.
- RHEL 4 / 5 / 6 : rpm (RHSA-2011-1349) (56383):
  - Update the affected packages.
- RHEL 4 : xorg-x11 (RHSA-2011-1360) (56411):
  - Update the affected packages.

- RHEL 4 / 5 / 6 : freetype (RHSA-2011-1455) (56859):
  - Update the affected packages.
- RHEL 4 : bind (RHSA-2011-1496) (56975):
  - Update the affected packages.
- RHEL 4 / 5 : perl (RHSA-2011-1797) (57053):
  - Update the affected perl and / or perl-suidperl packages.
- RHEL 4 / 5 : krb5 (RHSA-2011-1851) (57408):
  - Update the affected packages.
- RHEL 4 : libxml2 (RHSA-2012-0016) (57491):
  - Update the affected libxml2, libxml2-devel and / or libxml2-python packages.
- RHEL 4 : openssl (RHSA-2012-0086) (57789):
  - Update the affected openssl, openssl-devel and / or openssl-perl packages.
- RHEL 4 : glibc (RHSA-2012-0125) (57928):
  - Update the affected packages.
- RHEL 4 / 5 / 6 : libpng (RHSA-2012-0317) (58068):
  - Update the affected packages.

Remediation Plan for 172.26.48.50

You need to take the following 101 actions:

- RHEL 3 / 4 / 5 : vnc (RHSA-2009-0261) (35654):
  - Update the affected vnc and / or vnc-server packages.
- RHEL 5 : lcms (RHSA-2009-0339) (35970):
  - Update the affected lcms, lcms-devel and / or python-lcms packages.
- RHEL 5 : glib2 (RHSA-2009-0336) (36015):
  - Update the affected glib2 and / or glib2-devel packages.
- RHEL 5 : gstreamer-plugins-base (RHSA-2009-0352) (36099):
  - Update the affected gstreamer-plugins-base and / or gstreamer-plugins-base-devel packages.
- RHEL 4 / 5 : device-mapper-multipath (RHSA-2009-0411) (36115):
  - Update the affected device-mapper-multipath and / or kpartx packages.
- RHEL 5 : udev (RHSA-2009-0427) (36177):
  - Update the affected libvolume*id, libvolume*id-devel and / or udev packages.
- RHEL 5 : giflib (RHSA-2009-0444) (37605):
  - Update the affected giflib, giflib-devel and / or giflib-utils packages.
- RHEL 4 / 5 : libwmf (RHSA-2009-0457) (38659):
  - Update the affected libwmf and / or libwmf-devel packages.
- RHEL 5 : ipsec-tools (RHSA-2009-1036) (38819):
  - Update the affected ipsec-tools package.
- RHEL 5 : dnsmasq (RHSA-2009-1238) (40834):
  - Update the affected dnsmasq package.
- RHEL 5 : gdm (RHSA-2009-1364) (40840):
  - Update the affected gdm and / or gdm-docs packages.
- RHEL 3 / 4 / 5 : newt (RHSA-2009-1463) (41620):
  - Update the affected newt and / or newt-devel packages.
- RHEL 5 : openssh (RHSA-2009-1470) (41951):
  - Update the affected packages.
- RHEL 4 / 5 : samba (RHSA-2009-1529) (42286):
  - Update the affected packages.
- RHEL 3 / 4 / 5 : wget (RHSA-2009-1549) (42359):
  - Update the affected wget package.
- RHEL 5 : acpid (RHSA-2009-1642) (43047):
  - Update the affected acpid package.
- RHEL 4 / 5 : ntp (RHSA-2009-1648) (43080):
  - Update the affected ntp package.
- RHEL 4 / 5 : PyXML (RHSA-2010-0002) (43627):
  - Update the affected PyXML package.
- RHEL 4 / 5 : gd (RHSA-2010-0003) (43628):
  - Update the affected gd, gd-devel and / or gd-progs packages.
- RHEL 3 / 4 / 5 : gzip (RHSA-2010-0061) (44104):
  - Update the affected gzip package.
- RHEL 4 / 5 : tar (RHSA-2010-0141) (46264):
  - Update the affected tar package.
- RHEL 5 : cpio (RHSA-2010-0144) (46267):
  - Update the affected cpio package.
- RHEL 5 : squid (RHSA-2010-0221) (46285):
  - Update the affected squid package.
- RHEL 5 : sendmail (RHSA-2010-0237) (46286):

    - Update the affected packages.
- RHEL 5 : pam_krb5 (RHSA-2010-0258) (46287):
    - Update the affected pam_krb5 package.
- RHEL 5 : nss_db (RHSA-2010-0347) (46297):
    - Update the affected nss_db package.
- RHEL 4 / 5 : kdebase (RHSA-2010-0348) (46298):
    - Update the affected kdebase and / or kdebase-devel packages.
- RHEL 5 : rhn-client-tools (RHSA-2010-0449) (46780):
    - Update the affected packages.
- RHEL 4 / 5 : perl-Archive-Tar (RHSA-2010-0505) (47871):
    - Update the affected perl-Archive-Tar package.
- RHEL 5 : pcsc-lite (RHSA-2010-0533) (47875):
    - Update the affected packages.
- RHEL 5 : lftp (RHSA-2010-0585) (48232):
    - Update the affected lftp package.
- RHEL 5 : dbus-glib (RHSA-2010-0616) (48313):
    - Update the affected packages.
- RHEL 3 / 4 / 5 : bzip2 (RHSA-2010-0703) (49301):
    - Update the affected bzip2, bzip2-devel and / or bzip2-libs packages.
- RHEL 5 : poppler (RHSA-2010-0749) (49796):
    - Update the affected poppler, poppler-devel and / or poppler-utils packages.
- RHEL 5 : pam (RHSA-2010-0819) (50447):
    - Update the affected pam and / or pam-devel packages.
- RHEL 5 : gcc (RHSA-2011-0025) (51523):
    - Update the affected packages.
- RHEL 5 / 6 : hplip (RHSA-2011-0154) (51563):
    - Update the affected packages.
- RHEL 4 / 5 / 6 : libuser (RHSA-2011-0170) (51590):
    - Update the affected packages.
- RHEL 4 / 5 / 6 : pango (RHSA-2011-0180) (51811):
    - Update the affected packages.
- RHEL 5 / 6 : logwatch (RHSA-2011-0324) (52578):
    - Update the affected logwatch package.
- RHEL 5 : openldap (RHSA-2011-0346) (52627):
    - Update the affected packages.
- RHEL 5 / 6 : xorg-x11-server-utils (RHSA-2011-0433) (53371):
    - Update the affected xorg-x11-server-utils and / or xorg-x11-server-utils-debuginfo packages.
- RHEL 5 : avahi (RHSA-2011-0436) (53400):
    - Update the affected packages.
- RHEL 4 / 5 / 6 : apr (RHSA-2011-0844) (54932):
    - Update the affected packages.
- RHEL 5 : bash (RHSA-2011-1073) (55646):
    - Update the affected bash package.
- RHEL 4 / 5 : foomatic (RHSA-2011-1109) (55755):
    - Update the affected foomatic package.
- RHEL 5 / 6 : dbus (RHSA-2011-1132) (55809):
    - Update the affected packages.
- RHEL 5 / 6 : libXfont (RHSA-2011-1154) (55824):
    - Update the affected libXfont, libXfont-debuginfo and / or libXfont-devel packages.
- RHEL 4 / 5 / 6 : dovecot (RHSA-2011-1187) (55917):
    - Update the affected packages.
- RHEL 4 / 5 : system-config-printer (RHSA-2011-1196) (55965):
    - Update the affected system-config-printer, system-config-printer-gui and / or system-config-printer-libs packages.
- RHEL 5 : pango (RHSA-2011-1326) (56253):
    - Update the affected pango and / or pango-devel packages.
- RHEL 4 / 5 / 6 : kdelibs and kdelibs3 (RHSA-2011-1385) (56561):
    - Update the affected packages.
- RHEL 4 / 5 : netpbm (RHSA-2011-1811) (57081):
    - Update the affected netpbm, netpbm-devel and / or netpbm-progs packages.
- RHEL 4 / 5 / 6 : firefox (RHSA-2012-0079) (57760):
    - Update the affected packages.
- RHEL 4 / 5 / 6 : libvorbis (RHSA-2012-0136) (57957):
    - Update the affected packages.
- RHEL 5 / 6 : xulrunner (RHSA-2012-0143) (57995):
    - Update the affected xulrunner, xulrunner-debuginfo and / or xulrunner-devel packages.
- RHEL 5 : kexec-tools (RHSA-2012-0152) (58053):
    - Update the affected kexec-tools package.

- RHEL 5 : sos (RHSA-2012-0153) (58054):
  - Update the affected sos package.
- RHEL 5 : xorg-x11-server (RHSA-2012-0303) (58057):
  - Update the affected packages.
- RHEL 5 : vixie-cron (RHSA-2012-0304) (58058):
  - Update the affected vixie-cron package.
- RHEL 5 : krb5 (RHSA-2012-0306) (58060):
  - Update the affected packages.
- RHEL 5 : util-linux (RHSA-2012-0307) (58061):
  - Update the affected util-linux package.
- RHEL 5 : busybox (RHSA-2012-0308) (58062):
  - Update the affected busybox and / or busybox-anaconda packages.
- RHEL 5 : nfs-utils (RHSA-2012-0310) (58064):
  - Update the affected nfs-utils package.
- RHEL 5 : initscripts (RHSA-2012-0312) (58066):
  - Update the affected initscripts package.
- RHEL 5 / 6 : rpm (RHSA-2012-0451) (58586):
  - Update the affected packages.
- RHEL 5 / 6 : samba (RHSA-2012-0465) (58672):
  - Update the affected packages.
- RHEL 5 / 6 : libpng (RHSA-2012-0523) (58882):
  - Update the affected packages.
- RHEL 5 : ImageMagick (RHSA-2012-0545) (59029):
  - Update the affected packages.
- RHEL 5 / 6 : expat (RHSA-2012-0731) (59491):
  - Update the affected expat, expat-debuginfo and / or expat-devel packages.
- RHEL 5 : python (RHSA-2012-0745) (59564):
  - Update the affected packages.
- RHEL 5 : php (RHSA-2012-1045) (59751):
  - Update the affected packages.
- RHEL 5 : nss and nspr (RHSA-2012-1090) (60010):
  - Update the affected packages.
- RHEL 5 : dhcp (RHSA-2012-1140) (61404):
  - Update the affected packages.
- RHEL 5 : sudo (RHSA-2012-1149) (61452):
  - Update the affected sudo package.
- RHEL 5 / 6 : libexif (RHSA-2012-1255) (62055):
  - Update the affected libexif, libexif-debuginfo and / or libexif-devel packages.
- RHEL 5 / 6 : ghostscript (RHSA-2012-1256) (62056):
  - Update the affected packages.
- RHEL 5 : postgresql (RHSA-2012-1264) (62089):
  - Update the affected packages.
- RHEL 5 / 6 : libxslt (RHSA-2012-1265) (62090):
  - Update the affected packages.
- RHEL 5 / 6 : bind (RHSA-2012-1363) (62543):
  - Update the affected packages.
- RHEL 5 / 6 : libtiff (RHSA-2012-1590) (63293):
  - Update the affected packages.
- RHEL 5 : quota (RHSA-2013-0120) (63403):
  - Update the affected quota package.
- RHEL 5 : tcl (RHSA-2013-0122) (63405):
  - Update the affected tcl, tcl-devel and / or tcl-html packages.
- RHEL 5 : OpenIPMI (RHSA-2013-0123) (63406):
  - Update the affected packages.
- RHEL 5 : net-snmp (RHSA-2013-0124) (63407):
  - Update the affected packages.
- RHEL 5 : httpd (RHSA-2013-0130) (63411):
  - Update the affected packages.
- RHEL 5 : gnome-vfs2 (RHSA-2013-0131) (63412):
  - Update the affected gnome-vfs2, gnome-vfs2-devel and / or gnome-vfs2-smb packages.
- RHEL 5 : autofs (RHSA-2013-0132) (63413):
  - Update the affected autofs package.
- RHEL 5 : gtk2 (RHSA-2013-0135) (63416):
  - Update the affected gtk2 and / or gtk2-devel packages.
- RHEL 5 : mysql (RHSA-2013-0180) (63663):
  - Update the affected packages.
- RHEL 5 / 6 : freetype (RHSA-2013-0216) (64390):
  - Update the affected packages.

- RHEL 5 / 6 : firefox (RHSA-2013-0271) (64696):
  - Update the affected packages.
- RHEL 5 / 6 : dbus-glib (RHSA-2013-0568) (64904):
  - Update the affected dbus-glib, dbus-glib-debuginfo and / or dbus-glib-devel packages.
- RHEL 5 / 6 : cups (RHSA-2013-0580) (64944):
  - Update the affected packages.
- RHEL 5 / 6 : libxml2 (RHSA-2013-0581) (64945):
  - Update the affected packages.
- RHEL 5 / 6 : openssl (RHSA-2013-0587) (65004):
  - Update the affected packages.
- RHEL 5 / 6 : gnutls (RHSA-2013-0588) (65005):
  - Update the affected packages.
- RHEL 5 / 6 : perl (RHSA-2013-0685) (65698):
  - Update the affected packages.
- RHEL 5 : kernel (RHSA-2013-0747) (65991):
  - Update the affected packages.
- RHEL 5 : glibc (RHSA-2013-0769) (66211):
  - Update the affected packages.
- RHEL 5 / 6 : curl (RHSA-2013-0771) (66213):
  - Update the affected packages.

Remediation Plan for 172.26.48.51

You need to take the following 100 actions:

- RHEL 3 / 4 / 5 : vnc (RHSA-2009-0261) (35654):
  - Update the affected vnc and / or vnc-server packages.
- RHEL 4 / 5 : libsoup (RHSA-2009-0344) (35944):
  - Update the affected packages.
- RHEL 4 / 5 : evolution-data-server (RHSA-2009-0354) (35945):
  - Update the affected packages.
- RHEL 5 : lcms (RHSA-2009-0339) (35970):
  - Update the affected lcms, lcms-devel and / or python-lcms packages.
- RHEL 5 : glib2 (RHSA-2009-0336) (36015):
  - Update the affected glib2 and / or glib2-devel packages.
- RHEL 5 : gstreamer-plugins-base (RHSA-2009-0352) (36099):
  - Update the affected gstreamer-plugins-base and / or gstreamer-plugins-base-devel packages.
- RHEL 4 / 5 : device-mapper-multipath (RHSA-2009-0411) (36115):
  - Update the affected device-mapper-multipath and / or kpartx packages.
- RHEL 5 : udev (RHSA-2009-0427) (36177):
  - Update the affected libvolume*id, libvolume*id-devel and / or udev packages.
- RHEL 5 : giflib (RHSA-2009-0444) (37605):
  - Update the affected giflib, giflib-devel and / or giflib-utils packages.
- RHEL 4 / 5 : libwmf (RHSA-2009-0457) (38659):
  - Update the affected libwmf and / or libwmf-devel packages.
- RHEL 5 : ipsec-tools (RHSA-2009-1036) (38819):
  - Update the affected ipsec-tools package.
- RHEL 5 : gstreamer-plugins-good (RHSA-2009-1123) (39526):
  - Update the affected gstreamer-plugins-good and / or gstreamer-plugins-good-devel packages.
- RHEL 5 : dnsmasq (RHSA-2009-1238) (40834):
  - Update the affected dnsmasq package.
- RHEL 5 : gdm (RHSA-2009-1364) (40840):
  - Update the affected gdm and / or gdm-docs packages.
- RHEL 3 / 4 / 5 : fetchmail (RHSA-2009-1427) (40901):
  - Update the affected fetchmail package.
- RHEL 4 / 5 : neon (RHSA-2009-1452) (41031):
  - Update the affected neon and / or neon-devel packages.
- RHEL 3 / 4 / 5 : newt (RHSA-2009-1463) (41620):
  - Update the affected newt and / or newt-devel packages.
- RHEL 5 : openssh (RHSA-2009-1470) (41951):
  - Update the affected packages.
- RHEL 4 / 5 : samba (RHSA-2009-1529) (42286):
  - Update the affected packages.
- RHEL 3 / 4 / 5 : wget (RHSA-2009-1549) (42359):
  - Update the affected wget package.
- RHEL 5 : acpid (RHSA-2009-1642) (43047):
  - Update the affected acpid package.
- RHEL 3 / 4 / 5 : libtool (RHSA-2009-1646) (43078):

    - Update the affected packages.
- RHEL 4 / 5 : ntp (RHSA-2009-1648) (43080):
    - Update the affected ntp package.
- RHEL 4 / 5 : PyXML (RHSA-2010-0002) (43627):
    - Update the affected PyXML package.
- RHEL 4 / 5 : gd (RHSA-2010-0003) (43628):
    - Update the affected gd, gd-devel and / or gd-progs packages.
- RHEL 3 / 4 / 5 : gzip (RHSA-2010-0061) (44104):
    - Update the affected gzip package.
- RHEL 4 / 5 : tar (RHSA-2010-0141) (46264):
    - Update the affected tar package.
- RHEL 5 : cpio (RHSA-2010-0144) (46267):
    - Update the affected cpio package.
- RHEL 5 : brltty (RHSA-2010-0181) (46283):
    - Update the affected brlapi, brlapi-devel and / or brltty packages.
- RHEL 5 : sendmail (RHSA-2010-0237) (46286):
    - Update the affected packages.
- RHEL 5 : nss_db (RHSA-2010-0347) (46297):
    - Update the affected nss_db package.
- RHEL 5 : rhn-client-tools (RHSA-2010-0449) (46780):
    - Update the affected packages.
- RHEL 5 : pcsc-lite (RHSA-2010-0533) (47875):
    - Update the affected packages.
- RHEL 5 : lftp (RHSA-2010-0585) (48232):
    - Update the affected lftp package.
- RHEL 5 : dbus-glib (RHSA-2010-0616) (48313):
    - Update the affected packages.
- RHEL 3 / 4 / 5 : bzip2 (RHSA-2010-0703) (49301):
    - Update the affected bzip2, bzip2-devel and / or bzip2-libs packages.
- RHEL 5 : poppler (RHSA-2010-0749) (49796):
    - Update the affected poppler, poppler-devel and / or poppler-utils packages.
- RHEL 5 : pam (RHSA-2010-0819) (50447):
    - Update the affected pam and / or pam-devel packages.
- RHEL 5 : gcc (RHSA-2011-0025) (51523):
    - Update the affected packages.
- RHEL 5 / 6 : hplip (RHSA-2011-0154) (51563):
    - Update the affected packages.
- RHEL 4 / 5 / 6 : libuser (RHSA-2011-0170) (51590):
    - Update the affected packages.
- RHEL 4 / 5 / 6 : pango (RHSA-2011-0180) (51811):
    - Update the affected packages.
- RHEL 5 / 6 : logwatch (RHSA-2011-0324) (52578):
    - Update the affected logwatch package.
- RHEL 4 / 5 / 6 : vsftpd (RHSA-2011-0337) (52608):
    - Update the affected vsftpd and / or vsftpd-debuginfo packages.
- RHEL 5 : openldap (RHSA-2011-0346) (52627):
    - Update the affected packages.
- RHEL 5 / 6 : xorg-x11-server-utils (RHSA-2011-0433) (53371):
    - Update the affected xorg-x11-server-utils and / or xorg-x11-server-utils-debuginfo packages.
- RHEL 5 : avahi (RHSA-2011-0436) (53400):
    - Update the affected packages.
- RHEL 5 : bash (RHSA-2011-1073) (55646):
    - Update the affected bash package.
- RHEL 4 / 5 : foomatic (RHSA-2011-1109) (55755):
    - Update the affected foomatic package.
- RHEL 5 / 6 : dbus (RHSA-2011-1132) (55809):
    - Update the affected packages.
- RHEL 5 / 6 : libXfont (RHSA-2011-1154) (55824):
    - Update the affected libXfont, libXfont-debuginfo and / or libXfont-devel packages.
- RHEL 4 / 5 : system-config-printer (RHSA-2011-1196) (55965):
    - Update the affected system-config-printer, system-config-printer-gui and / or system-config-printer-libs packages.
- RHEL 5 : pango (RHSA-2011-1326) (56253):
    - Update the affected pango and / or pango-devel packages.
- RHEL 4 / 5 : netpbm (RHSA-2011-1811) (57081):
    - Update the affected netpbm, netpbm-devel and / or netpbm-progs packages.
- RHEL 4 / 5 / 6 : firefox (RHSA-2012-0079) (57760):
    - Update the affected packages.

- RHEL 4 / 5 / 6 : libvorbis (RHSA-2012-0136) (57957):
  - Update the affected packages.
- RHEL 5 / 6 : xulrunner (RHSA-2012-0143) (57995):
  - Update the affected xulrunner, xulrunner-debuginfo and / or xulrunner-devel packages.
- RHEL 5 : kexec-tools (RHSA-2012-0152) (58053):
  - Update the affected kexec-tools package.
- RHEL 5 : sos (RHSA-2012-0153) (58054):
  - Update the affected sos package.
- RHEL 5 : xorg-x11-server (RHSA-2012-0303) (58057):
  - Update the affected packages.
- RHEL 5 : vixie-cron (RHSA-2012-0304) (58058):
  - Update the affected vixie-cron package.
- RHEL 5 : krb5 (RHSA-2012-0306) (58060):
  - Update the affected packages.
- RHEL 5 : util-linux (RHSA-2012-0307) (58061):
  - Update the affected util-linux package.
- RHEL 5 : busybox (RHSA-2012-0308) (58062):
  - Update the affected busybox and / or busybox-anaconda packages.
- RHEL 5 : nfs-utils (RHSA-2012-0310) (58064):
  - Update the affected nfs-utils package.
- RHEL 5 : initscripts (RHSA-2012-0312) (58066):
  - Update the affected initscripts package.
- RHEL 5 / 6 : rpm (RHSA-2012-0451) (58586):
  - Update the affected packages.
- RHEL 5 / 6 : samba (RHSA-2012-0465) (58672):
  - Update the affected packages.
- RHEL 5 / 6 : libpng (RHSA-2012-0523) (58882):
  - Update the affected packages.
- RHEL 5 : ImageMagick (RHSA-2012-0545) (59029):
  - Update the affected packages.
- RHEL 5 / 6 : expat (RHSA-2012-0731) (59491):
  - Update the affected expat, expat-debuginfo and / or expat-devel packages.
- RHEL 5 : python (RHSA-2012-0745) (59564):
  - Update the affected packages.
- RHEL 5 : nss and nspr (RHSA-2012-1090) (60010):
  - Update the affected packages.
- RHEL 5 : dhcp (RHSA-2012-1140) (61404):
  - Update the affected packages.
- RHEL 5 : sudo (RHSA-2012-1149) (61452):
  - Update the affected sudo package.
- RHEL 5 / 6 : libexif (RHSA-2012-1255) (62055):
  - Update the affected libexif, libexif-debuginfo and / or libexif-devel packages.
- RHEL 5 / 6 : ghostscript (RHSA-2012-1256) (62056):
  - Update the affected packages.
- RHEL 5 / 6 : libxslt (RHSA-2012-1265) (62090):
  - Update the affected packages.
- RHEL 5 / 6 : bind (RHSA-2012-1363) (62543):
  - Update the affected packages.
- RHEL 5 / 6 : libtiff (RHSA-2012-1590) (63293):
  - Update the affected packages.
- RHEL 5 : quota (RHSA-2013-0120) (63403):
  - Update the affected quota package.
- RHEL 5 : tcl (RHSA-2013-0122) (63405):
  - Update the affected tcl, tcl-devel and / or tcl-html packages.
- RHEL 5 : OpenIPMI (RHSA-2013-0123) (63406):
  - Update the affected packages.
- RHEL 5 : net-snmp (RHSA-2013-0124) (63407):
  - Update the affected packages.
- RHEL 5 : gnome-vfs2 (RHSA-2013-0131) (63412):
  - Update the affected gnome-vfs2, gnome-vfs2-devel and / or gnome-vfs2-smb packages.
- RHEL 5 : autofs (RHSA-2013-0132) (63413):
  - Update the affected autofs package.
- RHEL 5 : gtk2 (RHSA-2013-0135) (63416):
  - Update the affected gtk2 and / or gtk2-devel packages.
- RHEL 5 : mysql (RHSA-2013-0180) (63663):
  - Update the affected packages.
- RHEL 5 / 6 : freetype (RHSA-2013-0216) (64390):
  - Update the affected packages.

- RHEL 5 / 6 : elinks (RHSA-2013-0250) (64565):
  - Update the affected elinks and / or elinks-debuginfo packages.
- RHEL 5 / 6 : firefox (RHSA-2013-0271) (64696):
  - Update the affected packages.
- RHEL 5 / 6 : dbus-glib (RHSA-2013-0568) (64904):
  - Update the affected dbus-glib, dbus-glib-debuginfo and / or dbus-glib-devel packages.
- RHEL 5 / 6 : cups (RHSA-2013-0580) (64944):
  - Update the affected packages.
- RHEL 5 / 6 : libxml2 (RHSA-2013-0581) (64945):
  - Update the affected packages.
- RHEL 5 / 6 : openssl (RHSA-2013-0587) (65004):
  - Update the affected packages.
- RHEL 5 / 6 : gnutls (RHSA-2013-0588) (65005):
  - Update the affected packages.
- RHEL 5 / 6 : perl (RHSA-2013-0685) (65698):
  - Update the affected packages.
- RHEL 5 : kernel (RHSA-2013-0747) (65991):
  - Update the affected packages.
- RHEL 5 : glibc (RHSA-2013-0769) (66211):
  - Update the affected packages.
- RHEL 5 / 6 : curl (RHSA-2013-0771) (66213):
  - Update the affected packages.

Remediation Plan for 172.26.48.52

You need to take the following 60 actions:

- RHEL 6 : bzip2 (RHSA-2010-0858) (50630):
  - Update the affected packages.
- RHEL 4 / 5 / 6 : libuser (RHSA-2011-0170) (51590):
  - Update the affected packages.
- RHEL 4 / 5 / 6 : pango (RHSA-2011-0180) (51811):
  - Update the affected packages.
- RHEL 6 : pango (RHSA-2011-0309) (52493):
  - Update the affected pango, pango-debuginfo and / or pango-devel packages.
- RHEL 6 : libcgroup (RHSA-2011-0320) (52542):
  - Update the affected packages.
- RHEL 6 : rsync (RHSA-2011-0390) (53204):
  - Update the affected rsync and / or rsync-debuginfo packages.
- RHEL 6 : logrotate (RHSA-2011-0407) (53246):
  - Update the affected logrotate and / or logrotate-debuginfo packages.
- RHEL 6 : policycoreutils (RHSA-2011-0414) (53293):
  - Update the affected packages.
- RHEL 6 : polkit (RHSA-2011-0455) (53500):
  - Update the affected packages.
- RHEL 6 : sssd (RHSA-2011-0560) (54594):
  - Update the affected packages.
- RHEL 6 : avahi (RHSA-2011-0779) (54600):
  - Update the affected packages.
- RHEL 4 / 5 / 6 : postfix (RHSA-2011-0843) (54931):
  - Update the affected packages.
- RHEL 6 : system-config-firewall (RHSA-2011-0953) (55616):
  - Update the affected packages.
- RHEL 6 : libsndfile (RHSA-2011-1084) (55636):
  - Update the affected libsndfile, libsndfile-debuginfo and / or libsndfile-devel packages.
- RHEL 6 : rsyslog (RHSA-2011-1247) (56047):
  - Update the affected packages.
- RHEL 6 : kexec-tools (RHSA-2011-1532) (57013):
  - Update the affected kexec-tools and / or kexec-tools-debuginfo packages.
- RHEL 6 : nfs-utils (RHSA-2011-1534) (57015):
  - Update the affected nfs-utils and / or nfs-utils-debuginfo packages.
- RHEL 6 : libcap (RHSA-2011-1694) (57020):
  - Update the affected libcap, libcap-debuginfo and / or libcap-devel packages.
- RHEL 6 : jasper (RHSA-2011-1807) (57054):
  - Update the affected packages.
- RHEL 4 / 5 / 6 : libvorbis (RHSA-2012-0136) (57957):
  - Update the affected packages.
- RHEL 5 / 6 : cvs (RHSA-2012-0321) (58083):

    - Update the affected cvs, cvs-debuginfo and / or cvs-inetd packages.
- RHEL 5 / 6 : systemtap (RHSA-2012-0376) (58298):
    - Update the affected packages.
- RHEL 6 : libtasn1 (RHSA-2012-0427) (58508):
    - Update the affected packages.
- RHEL 5 / 6 : rpm (RHSA-2012-0451) (58586):
    - Update the affected packages.
- RHEL 5 / 6 : libpng (RHSA-2012-0523) (58882):
    - Update the affected packages.
- RHEL 5 / 6 : samba and samba3x (RHSA-2012-0533) (58940):
    - Update the affected packages.
- RHEL 5 / 6 : expat (RHSA-2012-0731) (59491):
    - Update the affected expat, expat-debuginfo and / or expat-devel packages.
- RHEL 6 : python (RHSA-2012-0744) (59563):
    - Update the affected packages.
- RHEL 6 : busybox (RHSA-2012-0810) (59586):
    - Update the affected busybox and / or busybox-petitboot packages.
- RHEL 6 : cifs-utils (RHSA-2012-0902) (59596):
    - Update the affected cifs-utils and / or cifs-utils-debuginfo packages.
- RHEL 6 : sos (RHSA-2012-0958) (59598):
    - Update the affected sos package.
- RHEL 5 / 6 : sudo (RHSA-2012-1081) (59982):
    - Update the affected sudo and / or sudo-debuginfo packages.
- RHEL 6 : nss, nspr, and nss-util (RHSA-2012-1091) (60011):
    - Update the affected packages.
- RHEL 6 : openldap (RHSA-2012-1151) (61454):
    - Update the affected packages.
- RHEL 6 : glibc (RHSA-2012-1208) (61691):
    - Update the affected packages.
- RHEL 6 : dbus (RHSA-2012-1261) (62087):
    - Update the affected packages.
- RHEL 5 / 6 : libtiff (RHSA-2012-1590) (63293):
    - Update the affected packages.
- RHEL 6 : ipa (RHSA-2013-0188) (63675):
    - Update the affected packages.
- RHEL 5 / 6 : freetype (RHSA-2013-0216) (64390):
    - Update the affected packages.
- RHEL 5 / 6 : elinks (RHSA-2013-0250) (64565):
    - Update the affected elinks and / or elinks-debuginfo packages.
- RHEL 6 : dhcp (RHSA-2013-0504) (64755):
    - Update the affected packages.
- RHEL 6 : util-linux-ng (RHSA-2013-0517) (64765):
    - Update the affected packages.
- RHEL 6 : openssh (RHSA-2013-0519) (64766):
    - Update the affected packages.
- RHEL 6 : pam (RHSA-2013-0521) (64768):
    - Update the affected pam, pam-debuginfo and / or pam-devel packages.
- RHEL 6 : gdb (RHSA-2013-0522) (64769):
    - Update the affected gdb, gdb-debuginfo and / or gdb-gdbserver packages.
- RHEL 5 / 6 : dbus-glib (RHSA-2013-0568) (64904):
    - Update the affected dbus-glib, dbus-glib-debuginfo and / or dbus-glib-devel packages.
- RHEL 5 / 6 : cups (RHSA-2013-0580) (64944):
    - Update the affected packages.
- RHEL 5 / 6 : libxml2 (RHSA-2013-0581) (64945):
    - Update the affected packages.
- RHEL 5 / 6 : openssl (RHSA-2013-0587) (65004):
    - Update the affected packages.
- RHEL 5 / 6 : gnutls (RHSA-2013-0588) (65005):
    - Update the affected packages.
- RHEL 6 : nss-pam-ldapd (RHSA-2013-0590) (65007):
    - Update the affected nss-pam-ldapd and / or nss-pam-ldapd-debuginfo packages.
- RHEL 6 : sssd (RHSA-2013-0663) (65626):
    - Update the affected packages.
- RHEL 5 / 6 : perl (RHSA-2013-0685) (65698):
    - Update the affected packages.
- RHEL 6 : pixman (RHSA-2013-0687) (65714):
    - Update the affected pixman, pixman-debuginfo and / or pixman-devel packages.
- RHEL 6 : bind (RHSA-2013-0689) (65728):

    - Update the affected packages.
- RHEL 6 : krb5 (RHSA-2013-0748) (65992):
    - Update the affected packages.
- RHEL 6 : kernel (RHSA-2013-0744) (66192):
    - Update the affected packages.
- RHEL 5 / 6 : java-1.6.0-openjdk (RHSA-2013-0770) (66212):
    - Update the affected packages.
- RHEL 5 / 6 : curl (RHSA-2013-0771) (66213):
    - Update the affected packages.
- RHEL 6 : mysql (RHSA-2013-0772) (66225):
    - Update the affected packages.

Remediation Plan for 172.26.48.53

You need to take the following 97 actions:

- RHEL 6 : bzip2 (RHSA-2010-0858) (50630):
    - Update the affected packages.
- RHEL 6 : poppler (RHSA-2010-0859) (50631):
    - Update the affected packages.
- RHEL 4 / 5 / 6 : apr-util (RHSA-2010-0950) (51072):
    - Update the affected packages.
- RHEL 6 : libvpx (RHSA-2010-0999) (51354):
    - Update the affected packages.
- RHEL 6 : evince (RHSA-2011-0009) (51432):
    - Update the affected packages.
- RHEL 4 / 5 / 6 : libuser (RHSA-2011-0170) (51590):
    - Update the affected packages.
- RHEL 6 : webkitgtk (RHSA-2011-0177) (51672):
    - Update the affected packages.
- RHEL 4 / 5 / 6 : pango (RHSA-2011-0180) (51811):
    - Update the affected packages.
- RHEL 6 : pango (RHSA-2011-0309) (52493):
    - Update the affected pango, pango-debuginfo and / or pango-devel packages.
- RHEL 6 : libcgroup (RHSA-2011-0320) (52542):
    - Update the affected packages.
- RHEL 6 : rsync (RHSA-2011-0390) (53204):
    - Update the affected rsync and / or rsync-debuginfo packages.
- RHEL 6 : gdm (RHSA-2011-0395) (53207):
    - Update the affected packages.
- RHEL 6 : logrotate (RHSA-2011-0407) (53246):
    - Update the affected logrotate and / or logrotate-debuginfo packages.
- RHEL 6 : policycoreutils (RHSA-2011-0414) (53293):
    - Update the affected packages.
- RHEL 5 / 6 : xorg-x11-server-utils (RHSA-2011-0433) (53371):
    - Update the affected xorg-x11-server-utils and / or xorg-x11-server-utils-debuginfo packages.
- RHEL 6 : polkit (RHSA-2011-0455) (53500):
    - Update the affected packages.
- RHEL 6 : sssd (RHSA-2011-0560) (54594):
    - Update the affected packages.
- RHEL 6 : avahi (RHSA-2011-0779) (54600):
    - Update the affected packages.
- RHEL 4 / 5 / 6 : postfix (RHSA-2011-0843) (54931):
    - Update the affected packages.
- RHEL 4 / 5 / 6 : apr (RHSA-2011-0844) (54932):
    - Update the affected packages.
- RHEL 6 : system-config-firewall (RHSA-2011-0953) (55616):
    - Update the affected packages.
- RHEL 6 : fuse (RHSA-2011-1083) (55635):
    - Update the affected packages.
- RHEL 6 : libsndfile (RHSA-2011-1084) (55636):
    - Update the affected libsndfile, libsndfile-debuginfo and / or libsndfile-devel packages.
- RHEL 6 : libsoup (RHSA-2011-1102) (55724):
    - Update the affected libsoup, libsoup-debuginfo and / or libsoup-devel packages.
- RHEL 5 / 6 : libXfont (RHSA-2011-1154) (55824):
    - Update the affected libXfont, libXfont-debuginfo and / or libXfont-devel packages.
- RHEL 6 : rsyslog (RHSA-2011-1247) (56047):
    - Update the affected packages.

- RHEL 6 : librsvg2 (RHSA-2011-1289) (56188):
  - Update the affected librsvg2, librsvg2-debuginfo and / or librsvg2-devel packages.
- RHEL 6 : NetworkManager (RHSA-2011-1338) (56304):
  - Update the affected packages.
- RHEL 6 : libarchive (RHSA-2011-1507) (56990):
  - Update the affected libarchive, libarchive-debuginfo and / or libarchive-devel packages.
- RHEL 6 : kexec-tools (RHSA-2011-1532) (57013):
  - Update the affected kexec-tools and / or kexec-tools-debuginfo packages.
- RHEL 6 : nfs-utils (RHSA-2011-1534) (57015):
  - Update the affected nfs-utils and / or nfs-utils-debuginfo packages.
- RHEL 6 : libcap (RHSA-2011-1694) (57020):
  - Update the affected libcap, libcap-debuginfo and / or libcap-devel packages.
- RHEL 6 : jasper (RHSA-2011-1807) (57054):
  - Update the affected packages.
- RHEL 5 / 6 : icu (RHSA-2011-1815) (57296):
  - Update the affected packages.
- RHEL 4 / 5 / 6 : firefox (RHSA-2012-0079) (57760):
  - Update the affected packages.
- RHEL 4 / 5 / 6 : libvorbis (RHSA-2012-0136) (57957):
  - Update the affected packages.
- RHEL 6 : texlive (RHSA-2012-0137) (57969):
  - Update the affected packages.
- RHEL 5 / 6 : xulrunner (RHSA-2012-0143) (57995):
  - Update the affected xulrunner, xulrunner-debuginfo and / or xulrunner-devel packages.
- RHEL 5 / 6 : cvs (RHSA-2012-0321) (58083):
  - Update the affected cvs, cvs-debuginfo and / or cvs-inetd packages.
- RHEL 5 / 6 : systemtap (RHSA-2012-0376) (58298):
  - Update the affected packages.
- RHEL 6 : libtasn1 (RHSA-2012-0427) (58508):
  - Update the affected packages.
- RHEL 5 / 6 : rpm (RHSA-2012-0451) (58586):
  - Update the affected packages.
- RHEL 5 / 6 : libpng (RHSA-2012-0523) (58882):
  - Update the affected packages.
- RHEL 5 / 6 : samba and samba3x (RHSA-2012-0533) (58940):
  - Update the affected packages.
- RHEL 5 / 6 : expat (RHSA-2012-0731) (59491):
  - Update the affected expat, expat-debuginfo and / or expat-devel packages.
- RHEL 6 : python (RHSA-2012-0744) (59563):
  - Update the affected packages.
- RHEL 6 : busybox (RHSA-2012-0810) (59586):
  - Update the affected busybox and / or busybox-petitboot packages.
- RHEL 6 : abrt, libreport, btparser, and python-meh (RHSA-2012-0841) (59589):
  - Update the affected packages.
- RHEL 6 : net-snmp (RHSA-2012-0876) (59592):
  - Update the affected packages.
- RHEL 6 : cifs-utils (RHSA-2012-0902) (59596):
  - Update the affected cifs-utils and / or cifs-utils-debuginfo packages.
- RHEL 6 : xorg-x11-server (RHSA-2012-0939) (59597):
  - Update the affected packages.
- RHEL 6 : sos (RHSA-2012-0958) (59598):
  - Update the affected sos package.
- RHEL 5 / 6 : sudo (RHSA-2012-1081) (59982):
  - Update the affected sudo and / or sudo-debuginfo packages.
- RHEL 6 : nss, nspr, and nss-util (RHSA-2012-1091) (60011):
  - Update the affected packages.
- RHEL 6 : openldap (RHSA-2012-1151) (61454):
  - Update the affected packages.
- RHEL 6 : gimp (RHSA-2012-1180) (61603):
  - Update the affected packages.
- RHEL 6 : glibc (RHSA-2012-1208) (61691):
  - Update the affected packages.
- RHEL 5 / 6 : libexif (RHSA-2012-1255) (62055):
  - Update the affected libexif, libexif-debuginfo and / or libexif-devel packages.
- RHEL 5 / 6 : ghostscript (RHSA-2012-1256) (62056):
  - Update the affected packages.
- RHEL 6 : dbus (RHSA-2012-1261) (62087):
  - Update the affected packages.

- RHEL 5 / 6 : libxslt (RHSA-2012-1265) (62090):
  - Update the affected packages.
- RHEL 6 : openjpeg (RHSA-2012-1283) (62169):
  - Update the affected packages.
- RHEL 6 : gegl (RHSA-2012-1455) (62897):
  - Update the affected gegl, gegl-debuginfo and / or gegl-devel packages.
- RHEL 6 : nspluginwrapper (RHSA-2012-1459) (62917):
  - Update the affected nspluginwrapper and / or nspluginwrapper-debuginfo packages.
- RHEL 6 : libproxy (RHSA-2012-1461) (62922):
  - Update the affected packages.
- RHEL 5 / 6 : libtiff (RHSA-2012-1590) (63293):
  - Update the affected packages.
- RHEL 6 : vino (RHSA-2013-0169) (63641):
  - Update the affected vino and / or vino-debuginfo packages.
- RHEL 6 : ipa (RHSA-2013-0188) (63675):
  - Update the affected packages.
- RHEL 5 / 6 : freetype (RHSA-2013-0216) (64390):
  - Update the affected packages.
- RHEL 6 : xorg-x11-drv-qxl (RHSA-2013-0218) (64392):
  - Update the affected xorg-x11-drv-qxl and / or xorg-x11-drv-qxl-debuginfo packages.
- RHEL 5 / 6 : elinks (RHSA-2013-0250) (64565):
  - Update the affected elinks and / or elinks-debuginfo packages.
- RHEL 5 / 6 : firefox (RHSA-2013-0271) (64696):
  - Update the affected packages.
- RHEL 6 : dnsmasq (RHSA-2013-0277) (64750):
  - Update the affected dnsmasq, dnsmasq-debuginfo and / or dnsmasq-utils packages.
- RHEL 6 : hplip (RHSA-2013-0500) (64752):
  - Update the affected packages.
- RHEL 6 : Core X11 clients (RHSA-2013-0502) (64753):
  - Update the affected packages.
- RHEL 6 : dhcp (RHSA-2013-0504) (64755):
  - Update the affected packages.
- RHEL 6 : httpd (RHSA-2013-0512) (64761):
  - Update the affected packages.
- RHEL 6 : util-linux-ng (RHSA-2013-0517) (64765):
  - Update the affected packages.
- RHEL 6 : openssh (RHSA-2013-0519) (64766):
  - Update the affected packages.
- RHEL 6 : pam (RHSA-2013-0521) (64768):
  - Update the affected pam, pam-debuginfo and / or pam-devel packages.
- RHEL 6 : gdb (RHSA-2013-0522) (64769):
  - Update the affected gdb, gdb-debuginfo and / or gdb-gdbserver packages.
- RHEL 5 / 6 : dbus-glib (RHSA-2013-0568) (64904):
  - Update the affected dbus-glib, dbus-glib-debuginfo and / or dbus-glib-devel packages.
- RHEL 5 / 6 : cups (RHSA-2013-0580) (64944):
  - Update the affected packages.
- RHEL 5 / 6 : libxml2 (RHSA-2013-0581) (64945):
  - Update the affected packages.
- RHEL 5 / 6 : openssl (RHSA-2013-0587) (65004):
  - Update the affected packages.
- RHEL 5 / 6 : gnutls (RHSA-2013-0588) (65005):
  - Update the affected packages.
- RHEL 6 : nss-pam-ldapd (RHSA-2013-0590) (65007):
  - Update the affected nss-pam-ldapd and / or nss-pam-ldapd-debuginfo packages.
- RHEL 6 : sssd (RHSA-2013-0663) (65626):
  - Update the affected packages.
- RHEL 5 / 6 : boost (RHSA-2013-0668) (65651):
  - Update the affected packages.
- RHEL 5 / 6 : perl (RHSA-2013-0685) (65698):
  - Update the affected packages.
- RHEL 6 : pixman (RHSA-2013-0687) (65714):
  - Update the affected pixman, pixman-debuginfo and / or pixman-devel packages.
- RHEL 6 : bind (RHSA-2013-0689) (65728):
  - Update the affected packages.
- RHEL 6 : krb5 (RHSA-2013-0748) (65992):
  - Update the affected packages.
- RHEL 6 : kernel (RHSA-2013-0744) (66192):
  - Update the affected packages.

- RHEL 5 / 6 : java-1.6.0-openjdk (RHSA-2013-0770) (66212):
  - Update the affected packages.
- RHEL 5 / 6 : curl (RHSA-2013-0771) (66213):
  - Update the affected packages.
- RHEL 6 : mysql (RHSA-2013-0772) (66225):
  - Update the affected packages.

Remediation Plan for 172.26.48.58

You need to take the following 1 actions:

- Apache HTTP Server httpOnly Cookie Information Disclosure (57792):
  - Upgrade to Apache version 2.2.22 or later.

Remediation Plan for 172.26.48.59

You need to take the following 1 actions:

- Samba 'AndX' Request Heap-Based Buffer Overflow (58327):
  - Apply patches from the vendor.

Remediation Plan for 172.26.48.61

You need to take the following 1 actions:

- Apache HTTP Server httpOnly Cookie Information Disclosure (57792):
  - Upgrade to Apache version 2.2.22 or later.

Remediation Plan for 172.26.48.64

You need to take the following 4 actions:

- OpenSSL SSL*OP*NETSCAPE*REUSE*CIPHER*CHANGE*BUG Session Resume Ciphersuite Downgrade Issue (51892):
  - Upgrade to OpenSSL 0.9.8q / 1.0.0.c or later, or contact your vendor for a patch.
- MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check) (58435):
  - Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 : http://technet.microsoft.com/en-us/security/bulletin/ms12-020
- Apache 2.2 < 2.2.24 Multiple Cross-Site Scripting Vulnerabilities (64912):
  - Either ensure that the affected modules are not in use or upgrade to Apache version 2.2.24 or later.
- PHP 5.3.x < 5.3.22 Multiple Vulnerabilities (64992):
  - Upgrade to PHP version 5.3.22 or later.

Remediation Plan for 172.26.48.68

You need to take the following 1 actions:

- MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check) (58435):
  - Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 : http://technet.microsoft.com/en-us/security/bulletin/ms12-020

Remediation Plan for 172.26.48.69

You need to take the following 1 actions:

- MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check) (58435):
  - Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 : http://technet.microsoft.com/en-us/security/bulletin/ms12-020

Remediation Plan for 172.26.48.71

You need to take the following 2 actions:

- MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)

(58435):
    - Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 : http://technet.microsoft.com/en-us/security/bulletin/ms12-020
- Oracle Database, April 2013 Critical Patch Update (65997):
    - Apply the April 2013 CPU.

Remediation Plan for 172.26.48.72

You need to take the following 1 actions:

- MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check) (58435):
    - Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 : http://technet.microsoft.com/en-us/security/bulletin/ms12-020

Remediation Plan for 172.26.48.73

You need to take the following 1 actions:

- MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check) (58435):
    - Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 : http://technet.microsoft.com/en-us/security/bulletin/ms12-020

Remediation Plan for 172.26.48.74

You need to take the following 1 actions:

- MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check) (58435):
    - Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 : http://technet.microsoft.com/en-us/security/bulletin/ms12-020

Remediation Plan for 172.26.48.75

You need to take the following 1 actions:

- MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check) (58435):
    - Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 : http://technet.microsoft.com/en-us/security/bulletin/ms12-020

Remediation Plan for 172.26.48.78

You need to take the following 2 actions:

- Apache 2.4 < 2.4.4 Multiple Cross-Site Scripting Vulnerabilities (64893):
    - Either ensure that the affected modules are not in use or upgrade to Apache version 2.4.4 or later.
- PHP 5.4.x < 5.4.12 Multiple Vulnerabilities (64993):
    - Upgrade to PHP version 5.4.12 or later.

Remediation Plan for 172.26.48.79

You need to take the following 2 actions:

- Apache 2.4 < 2.4.4 Multiple Cross-Site Scripting Vulnerabilities (64893):
    - Either ensure that the affected modules are not in use or upgrade to Apache version 2.4.4 or later.
- PHP 5.4.x < 5.4.12 Multiple Vulnerabilities (64993):
    - Upgrade to PHP version 5.4.12 or later.

Remediation Plan for 172.26.48.82

You need to take the following 1 actions:

- VMSA-2012-0009 : ESXi and ESX patches address critical security issues (uncredentialed check) (59447):
    - Apply the missing patches.

Remediation Plan for 172.26.48.84

You need to take the following 7 actions:

- Apple Xcode < 4.4 Multiple Vulnerabilities (Mac OS X) (61413):
  - Upgrade to Apple Xcode version 4.4 or greater.
- Viscosity ViscosityHelper Symlink Attack Local Privilege Escalation (65700):
  - Upgrade to Viscosity 1.4.2 or later.
- Firefox 19.x Multiple Vulnerabilities (Mac OS X) (65802):
  - Upgrade to Firefox 20 or later.
- Thunderbird 17.x < 17.0.5 Multiple Vulnerabilities (Mac OS X) (65803):
  - Upgrade to Thunderbird 17.0.5 or later.
- Adobe AIR for Mac 3.x <= 3.6.0.6090 Multiple Vulnerabilities (APSB13-11) (65911):
  - Upgrade to Adobe AIR 3.7.0.1530 or later.
- Flash Player for Mac <= 10.3.183.68 / 11.6.602.180 Multiple Vulnerabilities (APSB13-11) (65912):
  - Upgrade to Adobe Flash Player version 10.3.183.75 / 11.7.700.169 or later.
- Mac OS X : Java for Mac OS X 10.6 Update 15 (65998):
  - Upgrade to Java for Mac OS X 10.6 Update 15, which includes version 13.9.5 of the JavaVM Framework.

Remediation Plan for 172.26.48.85

You need to take the following 1 actions:

- Mac OS X : Safari < 6.0.4 SVG File Handling Arbitrary Code Execution (66000):
  - Upgrade to Safari 6.0.4 or later.

Remediation Plan for 172.26.48.86

You need to take the following 1 actions:

- Mac OS X : Safari < 6.0.4 SVG File Handling Arbitrary Code Execution (66000):
  - Upgrade to Safari 6.0.4 or later.

Remediation Plan for 172.26.48.89

You need to take the following 1 actions:

- MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check) (58435):
  - Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 : http://technet.microsoft.com/en-us/security/bulletin/ms12-020

Remediation Plan for 172.26.51.154

You need to take the following 3 actions:

- MS05-027: Vulnerability in SMB Could Allow Remote Code Execution (896422) (uncredentialed check) (18502):
  - Microsoft has released a set of patches for Windows 2000, XP and 2003 : http://technet.microsoft.com/en-us/security/bulletin/ms05-027
- MS05-039: Vulnerability in Plug and Play Service Could Allow Remote Code Execution (899588) (uncredentialed check) (19408):
  - Microsoft has released a set of patches for Windows 2000, XP and 2003 : http://technet.microsoft.com/en-us/security/bulletin/ms05-039
- MS05-051: Vulnerabilities in MSDTC Could Allow Remote Code Execution (902400) (uncredentialed check) (20008):
  - Microsoft has released a set of patches for Windows 2000, XP and 2003 : http://technet.microsoft.com/en-us/security/bulletin/ms05-051

Remediation Plan for 172.26.246.101

You need to take the following 1 actions:

- HP LeftHand Virtual SAN Appliance < 10.0 hydra Service Multiple Remote Code Execution Vulnerabilities (version check) (64633):
  - Upgrade to HP LeftHand Virtual SAN Appliance version 10.0 or later.

Remediation Plan for 172.26.246.102

You need to take the following 1 actions:

- HP LeftHand Virtual SAN Appliance < 10.0 hydra Service Multiple Remote Code Execution Vulnerabilities (version check) (64633):
    - Upgrade to HP LeftHand Virtual SAN Appliance version 10.0 or later.

Remediation Plan for 172.26.246.103

You need to take the following 1 actions:

- HP LeftHand Virtual SAN Appliance < 10.0 hydra Service Multiple Remote Code Execution Vulnerabilities (version check) (64633):
    - Upgrade to HP LeftHand Virtual SAN Appliance version 10.0 or later.

Remediation Plan for 172.26.246.104

You need to take the following 1 actions:

- HP LeftHand Virtual SAN Appliance < 10.0 hydra Service Multiple Remote Code Execution Vulnerabilities (version check) (64633):
    - Upgrade to HP LeftHand Virtual SAN Appliance version 10.0 or later.