



MCAFEE FOUNDSTONE FSL UPDATE

To better protect your environment McAfee has created this FSL check update for the Foundstone Product Suite. The following is a detailed summary of the new and updated checks included with this release.

NEW CHECKS

13252 - IBM solidDB rownum Condition Denial Of Service

Category: Windows Host Assessment -> Miscellaneous
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

BID: 51629

Description

A denial of service vulnerability is present in some versions of IBM SolidDB.

Observation

A denial of service vulnerability is present in some versions of IBM SolidDB.

The flaw is caused by an unspecified error when handling a SELECT statement containing a rownum condition with a subquery and can be exploited to cause the server to shutdown.

13236 - Oracle MySQL Server Multiple Vulnerabilities Prior To 5.0.95

Category: Windows Host Assessment -> Miscellaneous
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-0087, CVE-2012-0101, CVE-2012-0102, CVE-2012-0484, CVE-2012-0490, CVE-2012-0114, CVE-2012-0075

DISA IAVA: 2012-A-0011

BID: 51509

Description

Multiple vulnerabilities are present in some versions of Oracle MySQL.

Observation

Oracle MySQL is a widely used relational database management system.

Multiple vulnerabilities are present in some versions of Oracle MySQL. Multiple flaws are present due to error in multiple components in Oracle MySQL. Successful exploitation could allow an attacker to cause a denial of service.

13237 - Oracle MySQL Server Multiple Vulnerabilities Prior To 5.1.61

Category: Windows Host Assessment -> Miscellaneous
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-0113, CVE-2011-2262, CVE-2012-0116, CVE-2012-0118, CVE-2012-0087, CVE-2012-0101, CVE-2012-0102, CVE-2012-0115, CVE-2012-0119, CVE-2012-0120, CVE-2012-0484, CVE-2012-0485, CVE-2012-0490, CVE-2012-0112, CVE-2012-0114, CVE-2012-0492, CVE-2012-0075

DISA IAVA: 2012-A-0011

BID: 51509

Description

Multiple vulnerabilities are present in some versions of Oracle MySQL.

Observation

Oracle MySQL is a widely used relational database management system.

Multiple vulnerabilities are present in some versions of Oracle MySQL. Multiple flaws are present due to error in multiple components in Oracle MySQL. Successful exploitation could allow an attacker to gain sensitive information on affected target or cause a denial of service.

13238 - Oracle MySQL Server Multiple Vulnerabilities Prior To 5.5.20

Category: Windows Host Assessment -> Miscellaneous
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-0113, CVE-2011-2262, CVE-2012-0116, CVE-2012-0118, CVE-2012-0496, CVE-2012-0115, CVE-2012-0119, CVE-2012-0120, CVE-2012-0484, CVE-2012-0485, CVE-2012-0486, CVE-2012-0487, CVE-2012-0488, CVE-2012-0489, CVE-2012-0490, CVE-2012-0491, CVE-2012-0495, CVE-2012-0112, CVE-2012-0117, CVE-2012-0114, CVE-2012-0492, CVE-2012-0493, CVE-2012-0494, CVE-2012-0075

DISA IAVA: 2012-A-0011

BID: 51515

Description

Multiple vulnerabilities are present in some versions of Oracle MySQL.

Observation

Oracle MySQL is a widely used relational database management system.

Multiple vulnerabilities are present in some versions of Oracle MySQL. Multiple flaws are present due to error in multiple components in Oracle MySQL. Successful exploitation could allow an attacker to gain sensitive information on affected target or cause a denial of service.

13242 - McAfee Web Gateway Unspecified Cross-Site Scripting Vulnerability Prior To 7.1.5.2

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

Description

A cross site scripting vulnerability is present in some versions of McAfee Web Gateway.

Observation

McAfee Web Gateway is a web based security control designed to prevent web application attacks.

A cross site scripting vulnerability is present in some versions of McAfee Web Gateway. Unspecified user inputs are not properly sanitized before returning to the user. As a result, an attacker can execute arbitrary code in the context of a browser session of a user.

41850 - Red Hat Enterprise Linux RHSA-2012-0070 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2011-2686, CVE-2011-4815, CVE-2011-2705, CVE-2011-3009

Description

The scan detected that the host is missing the following update: RHSA-2012-0070

Observation

Updates often remediate critical security problems that should be quickly addressed. For more information see:

<https://rhn.redhat.com/errata/RHSA-2012-0070.html> RHEL5D i386 ruby-1.8.5-22.el5_7.1 ruby-docs-1.8.5-22.el5_7.1 ruby-tcltk-1.8.5-22.el5_7.1 ruby-libs-1.8.5-22.el5_7.1 ruby-ri-1.8.5-22.el5_7.1 ruby-debuginfo-1.8.5-22.el5_7.1 ruby-irb-1.8.5-22.el5_7.1 ruby-rdoc-1.8.5-22.el5_7.1 RHEL4AS i386 irb-1.8.1-18.el4 ruby-debuginfo-1.8.1-18.el4 ruby-tcltk-1.8.1-18.el4 ruby-libs-1.8.1-18.el4 ruby-1.8.1-18.el4 ruby-mode-1.8.1-18.el4 ruby-devel-1.8.1-18.el4 ruby-docs-1.8.1-18.el4 RHEL4ES i386 irb-1.8.1-18.el4 ruby-debuginfo-1.8.1-18.el4 ruby-tcltk-1.8.1-18.el4 ruby-libs-1.8.1-18.el4 ruby-1.8.1-18.el4 ruby-mode-1.8.1-18.el4 ruby-devel-1.8.1-18.el4 ruby-docs-1.8.1-18.el4 RHEL5S i386 ruby-ri-1.8.5-22.el5_7.1 ruby-1.8.5-22.el5_7.1 ruby-docs-1.8.5-22.el5_7.1 ruby-tcltk-1.8.5-22.el5_7.1 ruby-libs-1.8.5-22.el5_7.1 ruby-irb-1.8.5-22.el5_7.1 ruby-debuginfo-1.8.5-22.el5_7.1 ruby-devel-1.8.5-22.el5_7.1 ruby-mode-1.8.5-22.el5_7.1 ruby-rdoc-1.8.5-22.el5_7.1 RHEL4WS i386 irb-1.8.1-18.el4 ruby-debuginfo-1.8.1-18.el4 ruby-tcltk-1.8.1-18.el4 ruby-libs-1.8.1-18.el4 ruby-1.8.1-18.el4 ruby-mode-1.8.1-18.el4 ruby-devel-1.8.1-18.el4 ruby-docs-1.8.1-18.el4

41852 - Red Hat Enterprise Linux RHSA-2012-0071 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2011-2202, CVE-2011-1466, CVE-2011-4566, CVE-2011-0708, CVE-2011-4885

Description

The scan detected that the host is missing the following update: RHSA-2012-0071

Observation

Updates often remediate critical security problems that should be quickly addressed. For more information see:

<https://rhn.redhat.com/errata/RHSA-2012-0071.html> RHEL4AS i386 php-xmlrpc-4.3.9-3.35 php-domxml-4.3.9-3.35 php-debuginfo-4.3.9-3.35 php-ncurses-4.3.9-3.35 php-ldap-4.3.9-3.35 php-gd-4.3.9-3.35 php-pgsql-4.3.9-3.35 php-mbstring-4.3.9-3.35 php-devel-4.3.9-3.35 php-snmp-4.3.9-3.35 php-mysql-4.3.9-3.35 php-4.3.9-3.35 php-odbc-4.3.9-3.35 php-imap-4.3.9-3.35 php-pear-4.3.9-3.35 RHEL4ES i386 php-xmlrpc-4.3.9-3.35 php-domxml-4.3.9-3.35 php-debuginfo-4.3.9-3.35 php-ncurses-4.3.9-3.35 php-ldap-4.3.9-3.35 php-gd-4.3.9-3.35 php-pgsql-4.3.9-3.35 php-mbstring-4.3.9-3.35 php-devel-4.3.9-3.35 php-snmp-4.3.9-3.35 php-mysql-4.3.9-3.35 php-4.3.9-3.35 php-odbc-4.3.9-3.35 php-imap-4.3.9-3.35 php-pear-4.3.9-3.35 RHEL4WS i386 php-xmlrpc-4.3.9-3.35 php-domxml-4.3.9-3.35 php-debuginfo-4.3.9-3.35 php-ncurses-4.3.9-3.35 php-ldap-4.3.9-3.35 php-gd-4.3.9-3.35 php-pgsql-4.3.9-3.35 php-mbstring-4.3.9-3.35 php-devel-4.3.9-3.35 php-snmp-4.3.9-3.35 php-mysql-4.3.9-3.35 php-4.3.9-3.35 php-odbc-4.3.9-3.35 php-imap-4.3.9-3.35 php-pear-4.3.9-3.35

41853 - Red Hat Enterprise Linux RHSA-2012-0069 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2011-4815

Description

The scan detected that the host is missing the following update: RHSA-2012-0069

Observation

Updates often remediate critical security problems that should be quickly addressed. For more information see:

<https://rhn.redhat.com/errata/RHSA-2012-0069.html> RHEL6WS i386 ruby-debuginfo-1.8.7.352-4.el6_2 ruby-1.8.7.352-4.el6_2

ruby-libs-1.8.7.352-4.el6_2 ruby-irb-1.8.7.352-4.el6_2 RHEL6D i386 ruby-debuginfo-1.8.7.352-4.el6_2 ruby-1.8.7.352-4.el6_2
ruby-libs-1.8.7.352-4.el6_2 ruby-irb-1.8.7.352-4.el6_2 RHEL6S i386 ruby-debuginfo-1.8.7.352-4.el6_2 ruby-1.8.7.352-4.el6_2
ruby-libs-1.8.7.352-4.el6_2 ruby-irb-1.8.7.352-4.el6_2

85244 - CentOS 6 CESA-2012-0059 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS Patches and Hotfixes

Risk Level: Medium

Description

The scan detected that the host is missing the following update: CESA-2012-0059

Observation

Updates often remediate critical security problems that should be quickly addressed. For more information see:
<http://lists.centos.org/pipermail/centos-announce/2012-January/018396.html> CentOS 6 i686 openssl-1.0.0-20.el6_2.1 openssl-devel-1.0.0-20.el6_2.1 openssl-perl-1.0.0-20.el6_2.1 openssl-static-1.0.0-20.el6_2.1

85245 - CentOS 4, 5 CESA-2012-0070 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS Patches and Hotfixes

Risk Level: Medium

Description

The scan detected that the host is missing the following update: CESA-2012-0070

Observation

Updates often remediate critical security problems that should be quickly addressed. For more information see:
<http://lists.centos.org/pipermail/centos-announce/2012-January/018394.html> <http://lists.centos.org/pipermail/centos-announce/2012-January/018401.html> CentOS 4 i386 ruby-libs-1.8.1-18.el4 irb-1.8.1-18.el4 ruby-docs-1.8.1-18.el4 ruby-devel-1.8.1-18.el4 ruby-1.8.1-18.el4 ruby-mode-1.8.1-18.el4 ruby-tcltk-1.8.1-18.el4 CentOS 5 i386 ruby-ri-1.8.5-22.el5_7.1 ruby-1.8.5-22.el5_7.1 ruby-docs-1.8.5-22.el5_7.1 ruby-tcltk-1.8.5-22.el5_7.1 ruby-libs-1.8.5-22.el5_7.1 ruby-irb-1.8.5-22.el5_7.1 ruby-devel-1.8.5-22.el5_7.1 ruby-mode-1.8.5-22.el5_7.1 ruby-rdoc-1.8.5-22.el5_7.1

85246 - CentOS 6 CESA-2012-0062 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS Patches and Hotfixes

Risk Level: Medium

Description

The scan detected that the host is missing the following update: CESA-2012-0062

Observation

Updates often remediate critical security problems that should be quickly addressed. For more information see:
<http://lists.centos.org/pipermail/centos-announce/2012-January/018395.html> CentOS 6 i686 t1lib-static-5.1.2-6.el6_2.1 t1lib-apps-5.1.2-6.el6_2.1 t1lib-devel-5.1.2-6.el6_2.1 t1lib-5.1.2-6.el6_2.1

85247 - CentOS 6 CESA-2012-0058 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS Patches and Hotfixes

Risk Level: Medium

Description

The scan detected that the host is missing the following update: CESA-2012-0058

Observation

Updates often remediate critical security problems that should be quickly addressed. For more information see: <http://lists.centos.org/pipermail/centos-announce/2012-January/018397.html> CentOS 6 i686 glibc-devel-2.12-1.47.el6_2.5 glibc-2.12-1.47.el6_2.5 glibc-utils-2.12-1.47.el6_2.5 nscd-2.12-1.47.el6_2.5 glibc-static-2.12-1.47.el6_2.5 glibc-headers-2.12-1.47.el6_2.5 glibc-common-2.12-1.47.el6_2.5

85248 - CentOS 6 CESA-2012-0069 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS Patches and Hotfixes

Risk Level: Medium

Description

The scan detected that the host is missing the following update: CESA-2012-0069

Observation

Updates often remediate critical security problems that should be quickly addressed. For more information see: <http://lists.centos.org/pipermail/centos-announce/2012-January/018400.html> CentOS 6 i686 ruby-devel-1.8.7.352-4.el6_2 ruby-ri-1.8.7.352-4.el6_2 ruby-irb-1.8.7.352-4.el6_2 ruby-libs-1.8.7.352-4.el6_2 ruby-docs-1.8.7.352-4.el6_2 ruby-1.8.7.352-4.el6_2 ruby-static-1.8.7.352-4.el6_2 ruby-tcltk-1.8.7.352-4.el6_2 ruby-rdoc-1.8.7.352-4.el6_2

85249 - CentOS 4 CESA-2012-0071 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS Patches and Hotfixes

Risk Level: Medium

Description

The scan detected that the host is missing the following update: CESA-2012-0071

Observation

Updates often remediate critical security problems that should be quickly addressed. For more information see: <http://lists.centos.org/pipermail/centos-announce/2012-January/018402.html> CentOS 4 i386 php-xmlrpc-4.3.9-3.35 php-domxml-4.3.9-3.35 php-ncurses-4.3.9-3.35 php-ldap-4.3.9-3.35 php-gd-4.3.9-3.35 php-pgsql-4.3.9-3.35 php-mbstring-4.3.9-3.35 php-devel-4.3.9-3.35 php-snmp-4.3.9-3.35 php-mysql-4.3.9-3.35 php-4.3.9-3.35 php-odbc-4.3.9-3.35 php-imap-4.3.9-3.35 php-pear-4.3.9-3.35

86213 - Fedora Linux 15 FEDORA-2011-16284 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2011-0285, CVE-2011-1528, CVE-2011-1529, CVE-2011-1530, CVE-2011-0284, CVE-2011-1527, CVE-2011-0282, CVE-2011-0283, CVE-2011-0281, CVE-2010-4022

Description

The scan detected that the host is missing the following update: FEDORA-2011-16284

Observation

Updates often remediate critical security problems that should be quickly addressed. For more information see: <http://lists.fedoraproject.org/pipermail/package-announce/2012-January/072625.html> Fedora Core 15 krb5-1.9.2-4.fc15

90920 - Oracle Enterprise Linux ELSA-2012-0071 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2011-2202, CVE-2011-1466, CVE-2011-4566, CVE-2011-0708, CVE-2011-4885

Description

The scan detected that the host is missing the following update: ELSA-2012-0071

Observation

Updates often remediate critical security problems that should be quickly addressed. For more information see: <http://oss.oracle.com/pipermail/el-errata/2012-January/002580.html> OEL4 i386 php-xmlrpc-4.3.9-3.35 php-domxml-4.3.9-3.35 php-ncurses-4.3.9-3.35 php-ldap-4.3.9-3.35 php-gd-4.3.9-3.35 php-pgsql-4.3.9-3.35 php-mbstring-4.3.9-3.35 php-devel-4.3.9-3.35 php-snmp-4.3.9-3.35 php-mysql-4.3.9-3.35 php-4.3.9-3.35 php-odbc-4.3.9-3.35 php-imap-4.3.9-3.35 php-pear-4.3.9-3.35

90921 - Oracle Enterprise Linux ELSA-2012-0069 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2011-4815

Description

The scan detected that the host is missing the following update: ELSA-2012-0069

Observation

Updates often remediate critical security problems that should be quickly addressed. For more information see: <http://oss.oracle.com/pipermail/el-errata/2012-January/002577.html> OEL6 i386 ruby-devel-1.8.7.352-4.el6_2 ruby-ri-1.8.7.352-4.el6_2 ruby-irb-1.8.7.352-4.el6_2 ruby-libs-1.8.7.352-4.el6_2 ruby-docs-1.8.7.352-4.el6_2 ruby-static-1.8.7.352-4.el6_2 ruby-tcltk-1.8.7.352-4.el6_2 ruby-rdoc-1.8.7.352-4.el6_2

90922 - Oracle Enterprise Linux ELSA-2012-0070 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2011-4815, CVE-2011-3009

Description

The scan detected that the host is missing the following update: ELSA-2012-0070

Observation

Updates often remediate critical security problems that should be quickly addressed. For more information see: <http://oss.oracle.com/pipermail/el-errata/2012-January/002579.html> <http://oss.oracle.com/pipermail/el-errata/2012-January/002578.html> OEL5 i386 ruby-ri-1.8.5-22.el5_7.1 ruby-1.8.5-22.el5_7.1 ruby-docs-1.8.5-22.el5_7.1 ruby-tcltk-1.8.5-22.el5_7.1 ruby-libs-1.8.5-22.el5_7.1 ruby-irb-1.8.5-22.el5_7.1 ruby-devel-1.8.5-22.el5_7.1 ruby-mode-1.8.5-22.el5_7.1 ruby-rdoc-1.8.5-22.el5_7.1 OEL4 i386 ruby-libs-1.8.1-18.el4 irb-1.8.1-18.el4 ruby-docs-1.8.1-18.el4 ruby-devel-1.8.1-18.el4 ruby-1.8.1-18.el4 ruby-mode-1.8.1-18.el4 ruby-tcltk-1.8.1-18.el4

41851 - Red Hat Enterprise Linux RHSA-2012-0073 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes

Risk Level: Low

Description

The scan detected that the host is missing the following update: RHSA-2012-0073

Observation

Updates often remediate critical security problems that should be quickly addressed. For more information see: <https://rhn.redhat.com/errata/RHSA-2012-0073.html> RHEL4AS i386 redhat-release-4AS-10.7 RHEL4ES i386 redhat-release-4ES-10.7 RHEL4WS i386 redhat-release-4WS-10.7

50486 - Ubuntu Linux 11.10 USN-1351-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes

Risk Level: Low

CVE: CVE-2011-4406

Description

The scan detected that the host is missing the following update: USN-1351-1

Observation

Updates often remediate critical security problems that should be quickly addressed. For more information see: <https://lists.ubuntu.com/archives/ubuntu-security-announce/2012-January/001573.html> Ubuntu 11.10 accountsservice_0.6.14-1git1ubuntu1.1

50487 - Ubuntu Linux 10.04, 10.10, 11.04, 11.10 USN-1352-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes

Risk Level: Low

CVE: CVE-2011-4407

Description

The scan detected that the host is missing the following update: USN-1352-1

Observation

Updates often remediate critical security problems that should be quickly addressed. For more information see: <https://lists.ubuntu.com/archives/ubuntu-security-announce/2012-January/001572.html> Ubuntu 10.04 python-software-properties_0.75.10.2 Ubuntu 11.04 python-software-properties_0.80.9.1 Ubuntu 10.10 python-software-properties_0.76.7.1 Ubuntu 11.10 python-software-properties_0.81.13.3

58300 - Debian Linux 5.0, 6.0 DSA-2399-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes

Risk Level: Low

CVE: CVE-2011-2483, CVE-2011-4566, CVE-2012-0057, CVE-2011-1938, CVE-2011-4885

Description

The scan detected that the host is missing the following update: DSA-2399-1

Observation

Updates often remediate critical security problems that should be quickly addressed. For more information see: <http://lists.debian.org/debian-security-announce/2012/msg00023.html> Debian 5.0 i386 php5-mhash_5.2.6.dfsg.1-1+lenny14 php5-imap_5.2.6.dfsg.1-1+lenny14 php5-odbc_5.2.6.dfsg.1-1+lenny14 php5-tidy_5.2.6.dfsg.1-1+lenny14 php5-pspell_5.2.6.dfsg.1-1+lenny14 php5-common_5.2.6.dfsg.1-1+lenny14 php5-gmp_5.2.6.dfsg.1-1+lenny14 php5-snmp_5.2.6.dfsg.1-1+lenny14 php5-xmlrpc_5.2.6.dfsg.1-1+lenny14 php5-dev_5.2.6.dfsg.1-1+lenny14 php5-ldap_5.2.6.dfsg.1-1+lenny14 php5-curl_5.2.6.dfsg.1-1+lenny14 php5-dbg_5.2.6.dfsg.1-1+lenny14 php5-sqlite_5.2.6.dfsg.1-1+lenny14 php5-pgsql_5.2.6.dfsg.1-1+lenny14 php5-

sybase_5.2.6.dfsg.1-1+lenny14 php5-cli_5.2.6.dfsg.1-1+lenny14 libapache2-mod-php5filter_5.2.6.dfsg.1-1+lenny14 php5-mysql_5.2.6.dfsg.1-1+lenny14 libapache2-mod-php5_5.2.6.dfsg.1-1+lenny14 php5-recode_5.2.6.dfsg.1-1+lenny14 php5-xsl_5.2.6.dfsg.1-1+lenny14 php5-gd_5.2.6.dfsg.1-1+lenny14 php5-cgi_5.2.6.dfsg.1-1+lenny14 php5-mcrypt_5.2.6.dfsg.1-1+lenny14 php5-interbase_5.2.6.dfsg.1-1+lenny14 Debian 6.0 i386 php5-ldap_5.3.3-7+squeeze5 php5-sybase_5.3.3-7+squeeze5 php5-xsl_5.3.3-7+squeeze5 php5-cgi_5.3.3-7+squeeze5 libapache2-mod-php5_5.3.3-7+squeeze5 php5-pgsql_5.3.3-7+squeeze5 php5-xmlrpc_5.3.3-7+squeeze5 php5-sqlite_5.3.3-7+squeeze5 php5-curl_5.3.3-7+squeeze5 php5-snmp_5.3.3-7+squeeze5 php5-imap_5.3.3-7+squeeze5 php5-recode_5.3.3-7+squeeze5 php5-mcrypt_5.3.3-7+squeeze5 php5-odbc_5.3.3-7+squeeze5 php5-dbg_5.3.3-7+squeeze5 php5-gd_5.3.3-7+squeeze5 php5-intl_5.3.3-7+squeeze5 php5-pspell_5.3.3-7+squeeze5 libapache2-mod-php5filter_5.3.3-7+squeeze5 php5-interbase_5.3.3-7+squeeze5 php5-cli_5.3.3-7+squeeze5 php5-mysql_5.3.3-7+squeeze5 php5-gmp_5.3.3-7+squeeze5 php5-common_5.3.3-7+squeeze5 php5-tidy_5.3.3-7+squeeze5 php5-enchanted_5.3.3-7+squeeze5 php5-dev_5.3.3-7+squeeze5

58301 - Debian Linux 5.0, 6.0 DSA-2397-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes

Risk Level: Low

CVE: CVE-2011-4599

Description

The scan detected that the host is missing the following update: DSA-2397-1

Observation

Updates often remediate critical security problems that should be quickly addressed. For more information see: <http://lists.debian.org/debian-security-announce/2012/msg00021.html> Debian 5.0 i386 libicu38_3.8.1-3+lenny3 libicu-dev_3.8.1-3+lenny3 libicu38-dbg_3.8.1-3+lenny3 Debian 6.0 i386 libicu-dev_4.4.1-8 libicu44_4.4.1-8 libicu44-dbg_4.4.1-8

58302 - Debian Linux 5.0, 6.0 DSA-2399-2 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes

Risk Level: Low

CVE: CVE-2011-2483, CVE-2011-4566, CVE-2012-0057, CVE-2011-1938, CVE-2011-4885

Description

The scan detected that the host is missing the following update: DSA-2399-2

Observation

Updates often remediate critical security problems that should be quickly addressed. For more information see: <http://lists.debian.org/debian-security-announce/2012/msg00024.html> Debian 5.0 i386 php5-mhash_5.2.6.dfsg.1-1+lenny15 php5-pspell_5.2.6.dfsg.1-1+lenny15 libapache2-mod-php5_5.2.6.dfsg.1-1+lenny15 php5-odbc_5.2.6.dfsg.1-1+lenny15 php5-cli_5.2.6.dfsg.1-1+lenny15 php5-pgsql_5.2.6.dfsg.1-1+lenny15 php5-sybase_5.2.6.dfsg.1-1+lenny15 php5-xsl_5.2.6.dfsg.1-1+lenny15 php5-gd_5.2.6.dfsg.1-1+lenny15 php5-sqlite_5.2.6.dfsg.1-1+lenny15 php5-tidy_5.2.6.dfsg.1-1+lenny15 php5-mcrypt_5.2.6.dfsg.1-1+lenny15 php5-cgi_5.2.6.dfsg.1-1+lenny15 php5-xmlrpc_5.2.6.dfsg.1-1+lenny15 php5-dev_5.2.6.dfsg.1-1+lenny15 libapache2-mod-php5filter_5.2.6.dfsg.1-1+lenny15 php5-dbg_5.2.6.dfsg.1-1+lenny15 php5-common_5.2.6.dfsg.1-1+lenny15 php5-curl_5.2.6.dfsg.1-1+lenny15 php5-snmp_5.2.6.dfsg.1-1+lenny15 php5-mysql_5.2.6.dfsg.1-1+lenny15 php5-ldap_5.2.6.dfsg.1-1+lenny15 php5-gmp_5.2.6.dfsg.1-1+lenny15 php5-recode_5.2.6.dfsg.1-1+lenny15 php5-imap_5.2.6.dfsg.1-1+lenny15 php5-interbase_5.2.6.dfsg.1-1+lenny15 Debian 6.0 i386 php5-curl_5.3.3-7+squeeze6 php5-gd_5.3.3-7+squeeze6 php5-ldap_5.3.3-7+squeeze6 php5-interbase_5.3.3-7+squeeze6 php5-intl_5.3.3-7+squeeze6 php5-common_5.3.3-7+squeeze6 php5-imap_5.3.3-7+squeeze6 libapache2-mod-php5_5.3.3-7+squeeze6 php5-cgi_5.3.3-7+squeeze6 php5-snmp_5.3.3-7+squeeze6 php5-xsl_5.3.3-7+squeeze6 php5-mysql_5.3.3-7+squeeze6 php5-tidy_5.3.3-7+squeeze6 php5-dbg_5.3.3-7+squeeze6 php5-pgsql_5.3.3-7+squeeze6 php5-sybase_5.3.3-7+squeeze6 php5-mcrypt_5.3.3-7+squeeze6 php5-pspell_5.3.3-7+squeeze6 php5-xmlrpc_5.3.3-7+squeeze6 php5-cli_5.3.3-7+squeeze6 php5-sqlite_5.3.3-7+squeeze6 libapache2-mod-php5filter_5.3.3-7+squeeze6 php5-recode_5.3.3-7+squeeze6 php5-enchanted_5.3.3-7+squeeze6 php5-odbc_5.3.3-7+squeeze6 php5-gmp_5.3.3-7+squeeze6 php5-dev_5.3.3-7+squeeze6

58303 - Debian Linux 5.0, 6.0 DSA-2398-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes

Risk Level: Low

CVE: CVE-2011-3389, CVE-2012-0036

Description

The scan detected that the host is missing the following update: DSA-2398-1

Observation

Updates often remediate critical security problems that should be quickly addressed. For more information see: <http://lists.debian.org/debian-security-announce/2012/msg00022.html> Debian 5.0 i386 curl_7.18.2-8lenny6 libcurl4-openssl-dev_7.18.2-8lenny6 libcurl3-gnutls_7.18.2-8lenny6 libcurl3_7.18.2-8lenny6 libcurl3-dbg_7.18.2-8lenny6 libcurl4-gnutls-dev_7.18.2-8lenny6 Debian 6.0 i386 curl_7.21.0-2.1+squeeze1 libcurl3-gnutls_7.21.0-2.1+squeeze1 libcurl4-openssl-dev_7.21.0-2.1+squeeze1 libcurl4-gnutls-dev_7.21.0-2.1+squeeze1 libcurl3-dbg_7.21.0-2.1+squeeze1 libcurl3_7.21.0-2.1+squeeze1

86214 - Fedora Linux 16 FEDORA-2012-1028 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Low

CVE: CVE-2012-0809

Description

The scan detected that the host is missing the following update: FEDORA-2012-1028

Observation

Updates often remediate critical security problems that should be quickly addressed. For more information see: <http://lists.fedoraproject.org/pipermail/package-announce/2012-January/072651.html> Fedora Core 16 sudo-1.8.3p1-2.fc16

86215 - Fedora Linux 16 FEDORA-2012-0801 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Low

CVE: CVE-2012-0790

Description

The scan detected that the host is missing the following update: FEDORA-2012-0801

Observation

Updates often remediate critical security problems that should be quickly addressed. For more information see: <http://lists.fedoraproject.org/pipermail/package-announce/2012-January/072629.html> Fedora Core 16 smokeping-2.4.2-16.fc16

86216 - Fedora Linux 15 FEDORA-2011-17565 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Low

CVE: CVE-2011-3922

Description

The scan detected that the host is missing the following update: FEDORA-2011-17565

Observation

Updates often remediate critical security problems that should be quickly addressed. For more information see:
<http://lists.fedoraproject.org/pipermail/package-announce/2012-January/072653.html> Fedora Core 15 qt-4.7.4-10.fc15

86217 - Fedora Linux 15 FEDORA-2012-0813 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Low

CVE: CVE-2012-0790

Description

The scan detected that the host is missing the following update: FEDORA-2012-0813

Observation

Updates often remediate critical security problems that should be quickly addressed. For more information see:
<http://lists.fedoraproject.org/pipermail/package-announce/2012-January/072653.html> Fedora Core 15 smokeping-2.4.2-13.fc15

92871 - Mandriva Linux 2010.1, 2011.0 MDVSA-2012-011 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Mandriva Patches and Hotfixes

Risk Level: Low

CVE: CVE-2011-4108, CVE-2012-0050

Description

The scan detected that the host is missing the following update: MDVSA-2012-011

Observation

Updates often remediate critical security problems that should be quickly addressed. For more information see:
<http://lists.mandriva.com/security-announce/2012-01/msg00015.php> Mandriva Linux 2010.1 i586 libopenssl-engines1.0.0-1.0.0a-1.10 libopenssl1.0.0-devel-1.0.0a-1.10 openssl-1.0.0a-1.10 libopenssl0.9.8-0.9.8t-0.1 libopenssl1.0.0-1.0.0a-1.10 libopenssl1.0.0-static-devel-1.0.0a-1.10 Mandriva Linux 2011.0 i586 libopenssl-devel-1.0.0d-2.3 libopenssl-static-devel-1.0.0d-2.3 libopenssl1.0.0-1.0.0d-2.3 libopenssl-engines1.0.0-1.0.0d-2.3 openssl-1.0.0d-2.3

ENHANCED CHECKS

The following checks have been updated. Enhancements may include optimizations, changes that reflect new information on a vulnerability and anything else that improves upon an existing FSL check.

9670 - Wind River Systems VxWorks WDB Target Agent Debug Service Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous

Risk Level: High

DISA IAVA: 2010-B-0075

BID: 42114

Update Details

Recommendation is updated.

9743 - FutureSoft TFTP Server 2000 Remote Denial Of Service Vulnerability

Category: General Vulnerability Assessment -> Intrusive -> Miscellaneous

Risk Level: High

BID: 13908

[Update Details](#)

Recommendation is updated.

9805 - Microsoft Windows 'win32k!GreStretchBitInternal()' Local Denial Of Service Vulnerability

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

BID: 42496

[Update Details](#)

Recommendation is updated.

9815 - SMTP Server Too Long Line Denial Of Service Vulnerability

Category: General Vulnerability Assessment -> Intrusive -> Miscellaneous

Risk Level: High

[Update Details](#)

Recommendation is updated.

13024 - 3S CoDeSys Multiple Vulnerabilities

Category: Windows Host Assessment -> SCADA
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-5009

[Update Details](#)

Recommendation is updated.

13025 - Siemens SIMATIC WinCC Flexible Runtime Miniweb Denial of Service

Category: Windows Host Assessment -> SCADA
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-4879

BID: 50827

[Update Details](#)

Recommendation is updated.

CVE is updated.

13044 - Siemens SIMATIC WinCC Flexible Runtime HmiLoad Strings Remote Code Execution

Category: Windows Host Assessment -> SCADA
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-4875

BID: 50828

Update Details

Recommendation is updated.
CVE is updated.

13046 - Siemens SIMATIC WinCC Flexible Runtime HmiLoad Denial of Service

Category: Windows Host Assessment -> SCADA
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-4877

BID: 50828

Update Details

Recommendation is updated.
CVE is updated.

9671 - Microsoft Internet Explorer Frame Border Property Denial Of Service Vulnerability

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

BID: 41990

Update Details

Recommendation is updated.

9746 - PumpKIN TFTP Server Write Request Mode Field Denial Of Service Vulnerability

Category: General Vulnerability Assessment -> Intrusive -> Miscellaneous

Risk Level: Medium

CVE: CVE-2008-6791

BID: 31922

Update Details

Recommendation is updated.

9763 - (MS10-049) Microsoft Windows TLS/SSL Renegotiation Vulnerability (980436)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-3555

DISA IAVA: 2010-A-0108

Microsoft ID: MS10-049

Microsoft KB: 977377

BID: 36935

[Update Details](#)

Recommendation is updated.

9810 - RealVNC ClientCutText Message Remote Denial Of Service Vulnerability

Category: General Vulnerability Assessment -> Intrusive -> Miscellaneous

Risk Level: Medium

BID: 39895

[Update Details](#)

Recommendation is updated.

11650 - HP Data Protector Media Operations DBServer.exe Memory Corruption Remote Code Execution

Category: Windows Host Assessment -> Miscellaneous

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-4791

BID: 47004

[Update Details](#)

Recommendation is updated.

CVE is updated.

13009 - WordPress Simple Balance Theme s Parameter Cross Site Scripting Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> Web Server

Risk Level: Medium

[Update Details](#)

Recommendation is updated.

13026 - Siemens SIMATIC WinCC Flexible Runtime Miniweb Security Bypass

Category: General Vulnerability Assessment -> NonIntrusive -> SCADA

Risk Level: Medium

CVE: CVE-2011-4878

BID: 50827

[Update Details](#)

CVE is updated.

13045 - Siemens SIMATIC WinCC Flexible Runtime HmiLoad Security Bypass

Category: Windows Host Assessment -> SCADA
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-4876

BID: 50828

[Update Details](#)

CVE is updated.

13116 - WordPress UPM Polls Plugin PID SQL Injection Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> Web Server

Risk Level: Medium

BID: 51007

[Update Details](#)

Recommendation is updated.

94936 - SuSE SLES 11, 11 SP1 squid-5584 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2010-0639

[Update Details](#)

FASLScript is updated.

70014 - netbios-helpers.fasI3.inc

Category: General Vulnerability Assessment -> NonIntrusive -> Invalid Category

Risk Level: Informational

[Update Details](#)

FASLScript is updated.

70032 - mysql.fasI3.inc

Category: General Vulnerability Assessment -> NonIntrusive -> Invalid Category

Risk Level: Informational

Check Version: 1.2490

Update Details

FASLScript is updated.

70074 - mcafee.fasl3.inc

Category: General Vulnerability Assessment -> NonIntrusive -> Invalid Category

Risk Level: Informational

Update Details

FASLScript is updated.

HOW TO UPDATE

FS1000 APPLIANCE customers should follow the instructions for Enterprise/Professional customers, below. In addition, we strongly urge all appliance customers to authorize and install any Windows Update critical patches. The appliance will auto-download any critical updates but will wait for your explicit authorization before installing.

FOUNDSTONE ENTERPRISE and PROFESSIONAL customers may obtain these new scripts using the FSUpdate Utility by selecting "FoundScan Update" on the help menu. Make sure that you have a valid FSUpdate username and password. The new vulnerability scripts will be automatically included in your scans if you have selected that option by right-clicking the selected vulnerability category and checking the "Run New Checks" checkbox.

MANAGED SERVICE CUSTOMERS already have the newest update applied to their environment. The new vulnerability scripts will be automatically included when your scans are next scheduled, provided the Run New Scripts option has been turned on.

MCAFEE TECHNICAL SUPPORT

ServicePortal: <https://mysupport.mcafee.com>

Multi-National Phone Support available here:

<http://www.mcafee.com/us/about/contact/index.html>

Non-US customers - Select your country from the list of Worldwide Offices.

This email may contain confidential and privileged material for the sole use of the intended recipient. Any review or distribution by others is strictly prohibited. If you are not the intended recipient please contact the sender and delete all copies.

Copyright 2010 McAfee, Inc.

McAfee is a registered trademark of McAfee, Inc. and/or its affiliates