Information Warfare Center's Cyber Intelligence Report (CIR)

Author: Jeremy Martin, CISSP-ISSMP/ISSAP, CISM, CEH/LPT/CHFI, CREA/CEPT/CSSA/CCFE
www.informationwarfarecenter.com

September, 20 2012

The IWC CIR is a weekly OSINT resource focusing on advanced persistent threats and other digital dangers. APTs fit into a cybercrime category directed at business and political targets. Attack vectors include system compromise, social engineering, and even traditional espionage.

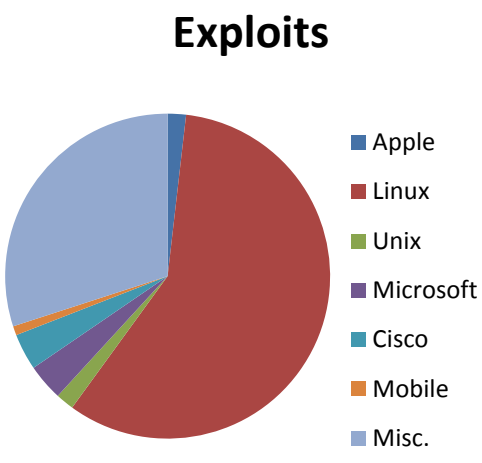
Top News

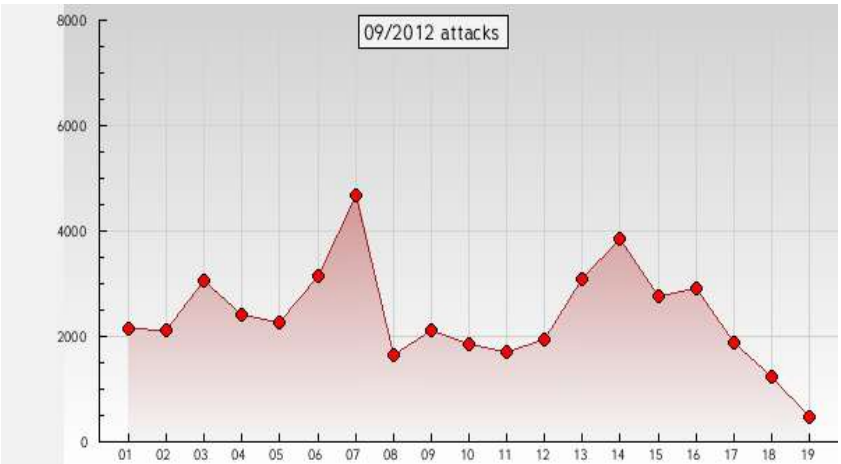
Technical Cyber Security Alert 2012-262A
Technical Cyber Security Alert 2012-262A - An unpatched use-after-free vulnerability in Microsoft Internet Explorer versions 7, 8, and 9 is being exploited in the wild. Microsoft has released Security Advisory 2757760 with mitigation techniques.

Gotcha
US Federal/State/Local government sites defaced/compromised this week (details later in this document)

- www.wmatc.gov
- greenbaywi.gov
- www.nmvb.ca.gov
- saltoncsd.ca.gov
- www.driveclean.ca.gov

Section	Page	Instances
In the News	2	44
Papers	5	9
Discussions	6	8
Advisories	7	122
Tools released	20	6
Exploits published	21	80
Vulnerable websites	22	12
Websites defaced	23	625





In the news:

Eastern Europe Hackers Bigger Threat Than Asian Cyber Snoops
Source V3

New Vicious UEFI Bootkit Vuln Found For Windows 8
Source The Register

IC3 Scam Alerts (September 19, 2012)

Two Executives Brief Congress on Threats to Nation
FBI Associate Deputy Director Kevin Perkins and Deputy Assistant Director of the Counterterrorism Division Michael Clancy testified before a Senate committee and subcommittee, respectively, on the increasingly complex threats facing our nation and how the FBI is continually evolving to counter those threats.

Online Poker Executive Pleads Guilty in Manhattan Federal Court to Money Laundering, Bank Fraud, and Internet Gambling Offenses
Sept. 19, 2012 - New York

Former CME Group Software Engineer Pleads Guilty to Stealing Globex Computer Trade Secrets While Planning to Improve Electronic Trading in China
Sept. 19, 2012 - Chicago

Homeland Threats and Agency Responses
Robert S. Mueller, III, Director, Statement Before the Senate Committee on Homeland Security and Governmental Affairs - Washington, D.C.

Columbia County Man Sentenced to Six Years in Federal Prison for Receiving Child Pornography Over the Internet
Sept. 18, 2012 - Jacksonville

Modesto Woman Pleads Guilty to Participating in Extensive Counterfeit Media Conspiracy
Sept. 17, 2012 - Sacramento

DC3.mil content:

Cyber Crime
Phishers continue to target legitimate websites
http://feedproxy.google.com/~r/HelpNetSecurity/~3/9nhds1t3YeU/secworld.php

Aspen Launches Cyber Crime Protection
http://bernews.com/2012/09/aspen-launches-cyber-crime-protection/

Cyber forensics to the fore
http://www.bangkokpost.com/tech/computer/312999/cyber-forensics-to-the-fore

Defence Headquarters Website Hacked
http://leadership.ng/nga/articles/35158/2012/09/19/defence_headquarters_website_hacked_cds.html

Attackers exploit unpatched Internet Explorer vulnerability
http://news.hitb.org/content/attackers-exploit-unpatched-internet-explorer-vulnerability

Flamer Malware Spied on Middle East for More Than Five Years
http://feeds.ziffdavisenterprise.com/~r/RSS/eweeksecurity/~3/LewX5OmmOrA/

New Iteration of TDSS/TDL-4 Botnet Uses Domain Fluxing to Avoid Detection
http://threatpost.com/en_us/blogs/new-iteration-tdsstdl-4-botnet-uses-domain-fluxing-avoid-detection-091712

Philippines inks Cyber Crime Prevention Act
http://www.infosecurity-magazine.com/view/28280/philippines-inks-cyber-crime-prevention-act

Pre-Infected PCs Expose Flaws In Global Supply Chain
http://www.huffingtonpost.com/2012/09/14/pre-infected-pcs-expose-risks_n_1884441.html

Strategy the best security defense: AFP
http://www.computerworld.com.au/article/436707/

Government
Freedom of (cyber) expression
http://www.asianjournal.com/editorial/5-editorial/17333-freedom-of-cyber-expression.html

Questions loom about Obamas cybersecurity plans
http://www.pcworld.com/article/2010001/questions-loom-about-obamas-cybersecurity-plans.html

When it comes to cybersecurity law, where do we draw the line on information
http://www.zdnet.com/when-it-comes-to-cybersecurity-law-where-do-we-draw-the-line-on-information-sharing-7000004415/

News, Technologies and Techniques
Real-world software security initiatives study
http://feedproxy.google.com/~r/HelpNetSecurity/~3/kumvHRj4130/secworld.php

German cybersecurity agency prods users to ditch IE
http://www.computerworld.com/s/article/9231414/

Invisible QR Codes Tackle Counterfeit Bank Notes
http://www.dfinews.com/news/invisible-qr-codes-tackle-counterfeit-bank-notes

Romanian POS Hackers Plead Guilty, Net $10 M from Scam
http://threatpost.com/en_us/blogs/romanian-pos-hackers-plead-guilty-net-10-m-scam-091812

Sequestration Could Hurt Cyber Defense Programs
http://www.dfinews.com/news/sequestration-could-hurt-cyber-defense-programs

Security Awareness Week Right Around the Corner
http://www.miamistudent.net/tech-tip/tech-tip-security-awareness-week-right-around-the-corner-1.2903663

Web developers application security sorely lacking
http://www.infosecurity-magazine.com/view/28320/web-developers-application-security-sorely-lacking/

A Start-up Figures Out Photoshopping Abuses
http://bits.blogs.nytimes.com/2012/09/18/taking-digital-image-forensics-out-of-the-lab-and-into-the-marketplace/

Coders Behind Flame Malware Left Incriminating Clues on Control Servers
http://www.dfinews.com/news/coders-behind-flame-malware-left-incriminating-clues-control-servers

Columbia Basin College to start cybersecurity program
http://www.thenewstribune.com/2012/09/18/2300175/columbia-basin-college-to-start.html

DMU to launch new cyber security centre
http://www.digitalforensicsmagazine.com/index.php?option=com_content&view=article&id=830:dmu-to-launch-new-cyber-security-centre&catid=1:latest-news&Itemid=50

Immediate Mobile Data Visualization for Field Investigators
http://www.dfinews.com/news/immediate-mobile-data-visualization-field-investigators

In 2012, cloud had fewer security incidents than on-premise IT
http://www.infosecurity-magazine.com/view/28050/in-2012-cloud-had-fewer-security-incidents-than-onpremise-it/

Mobile Devices are Important Sources of Digital Evidence That Can No Longer be Overlooked
http://www.equities.com/news/news-headline-story?dt=2012-09-17&val=485111&d=1&cat=headline

XRY v6.3.2 released
http://www.forensicfocus.com/News/article/sid=1935/

Security Alerts:
Bogus "Windows Email Security Update" emails lead to phishing
http://feedproxy.google.com/~r/HelpNetSecurity/~3/srs44-Fire0/secworld.php

Bank of America Hit by Cyber Attack
http://www.foxbusiness.com/industries/2012/09/18/bank-america-website-experiencing-sporadic-outages/

Cyber security professionals in high demand battling cyber weapons
http://www.tctimes.com/online_features/tech_talk_and_innovation/cyber-security-professionals-in-high-demand-battling-cyber-weapons/article_25be4d28-ef86-5cca-9349-4533e389d9c5.html

Passware Software Makes Windows Computers Accessible to Law Enforcement Exposing Login Passwords in Minutes
http://www.sacbee.com/2012/09/17/4827681/passware-software-makes-windows.html

TDSS Malware Infecting Fortune 500 Includes Evasion Tactic
http://feeds.ziffdavisenterprise.com/~r/RSS/eweeksecurity/~3/I3Xv8cupgLc/

Majority of companies suffered a web application security breach
http://feedproxy.google.com/~r/HelpNetSecurity/~3/OFkIKXwNqDI/secworld.php

Developer Warns Millions of Virgin Mobile Subscribers About Authentication Flaw
http://threatpost.com/en_us/blogs/developer-warns-millions-virgin-mobile-subscribers-about-authentication-flaw-091712

Papers:

How I DOS'ed My Bank
This is a brief whitepaper that discusses DTMF input processing and easy denial of service attack via phone lines against banking systems.

Intel SMEP Overview And Partial Bypass On Windows 8
This paper provides an overview of a new hardware security feature introduced by Intel and covers its support on Windows 8. Among the other common features it complicates vulnerability exploitation on a target system. But if these features are not properly configured all of them may become useless. This paper demonstrates a security flaw on x86 version of Windows 8 leading to a bypass of the SMEP security feature.

Hacking Android For Fun And Profit
This is a brief whitepaper with examples and information on hacking the Android platform from Google.

XSS Exploitation Via CHEF
This is a whitepaper discussing cross site scripting exploitation via CHEF. Written in Turkish.

Oracle Java Applet SunToolkit.getField Method Remote Code Execution
This document is an analysis of the Oracle Java Applet SunToolkit.getField remote code execution vulnerability as noted in CVE-2012-4681.

Taller De Inyecciones LDAP
This is a whitepaper called Taller De Inyecciones LDAP. It discusses various ways of attacking LDAP. Written in Spanish.

Chip And Skim: Cloning EMV Cards With The Pre-Play Attack
EMV, also known as "Chip and PIN", is the leading system for card payments world- wide. It is used throughout Europe and much of Asia, and is starting to be introduced in North America too. Payment cards contain a chip so they can execute an authentication protocol. This protocol requires point-of-sale (POS) terminals or ATMs to generate a nonce, called the unpredictable number, for each transaction to ensure it is fresh. The authors have discovered that some EMV implementers have merely used counters, timestamps or home-grown algorithms to supply this number. This exposes them to a "pre-play" attack which is indistinguishable from card cloning from the standpoint of the logs available to the card-issuing bank, and can be carried out even if it is impossible to clone a card physically (in the sense of extracting the key material and loading it into another card).

Detecting And Exploiting XSS With Xenotix XSS Exploit Framework
This is a whitepaper called Detecting and Exploiting XSS with Xenotix XSS Exploit Framework

An Introduction To ARM Exploitation
This is a brief whitepaper that discusses ARM exploitation and is based on work the author performed against Windows Mobile. Written in Turkish

The ZeroAccess Botnet: Mining and Fraud for Massive Financial Gain
Since our last paper on ZeroAccess, the authors have made significant changes. In this paper we will examine those changes and take a closer look at the ZeroAccess botnet itself, exploring its size, functionality and purpose. We will explain in detail how the peer-to-peer protocol works, what network traffic is created, and how the bot phones home during installation. Then we will examine the plugin files that the botnet downloads: what these files are, what they do and how they work.

Discussions

Hacking Banks using a Phone: Phonetic attack commands crash bank phone lines - Networks http://ow.ly/dLBLR
Started by Bikash Barai, CEO-iViZ, Cloud based Web Application Security Testing with "Zero False Positive Guarantee"

Automating and Interacting with Nessus via XML-RPC
Started by Nicholas Popovich, Security Centric IT Breadwinner

State-sponsored attack or not, that's the question
Started by Pierluigi Paganini, Chief Information Security Officer

Cybercrime evolution in North America and Western Europe
Started by Pierluigi Paganini, Chief Information Security Officer

pass the hash over @ MyExploitHQ
Started by Mark Smith, Senior Penetration Tester at evision-secure

The Browser Exploitation Framework (BeEF) – Part 2
Started by Robert Rodriguez, Director of Online Content at InfoSec Institute

Bank Fraud and ATM Security
Started by Robert Rodriguez, Director of Online Content at InfoSec Institute

The New Phishing Threat: Phishing Attacks!
Started by William Smith, IT Security Professional

Advisories for the week of September 20, 2012

Apache

Secunia Security Advisory 50541
Secunia Security Advisory - A security issue and a vulnerability have been reported in Apache HTTP Server, which can be exploited by malicious, local users to gain escalated privileges and by malicious people to conduct cross-site scripting attacks.

Secunia Security Advisory 50591
Secunia Security Advisory - Two vulnerabilities have been reported in Apache mod_pagespeed module, which can be exploited by malicious people to conduct cross-site scripting attacks and bypass certain security restrictions.

Apple

Secunia Security Advisory 50618
Secunia Security Advisory - Multiple vulnerabilities have been reported in Apple iTunes, which can be exploited by malicious people to compromise a user's system.

Apple Security Advisory 2012-09-12-1
Apple Security Advisory 2012-09-12-1 - iTunes 10.7 is now available and addresses multiple memory corruption issues in webkit.

Chrome

Secunia Security Advisory 50613
Secunia Security Advisory - Multiple vulnerabilities have been reported in Google Chrome for Android, which can be exploited by malicious people to disclose certain sensitive information and conduct cross-site scripting attacks.

Cisco

Secunia Security Advisory 50592
Secunia Security Advisory - A security issue has been reported in Cisco ASA-CX Context-Aware Security and Cisco Prime Security Manager (PRSM), which can be exploited by malicious people to cause a DoS (Denial of Service).

Secunia Security Advisory 50562
Secunia Security Advisory - A vulnerability has been reported in Cisco Unified Presence and Cisco Jabber XCP, which can be exploited by malicious people to cause a DoS (Denial of Service).

Cisco Security Advisory 20120912-asacx
Cisco Security Advisory - Cisco ASA-CX Context-Aware Security appliance and Cisco Prime Security Manager (PRSM) contain a denial of service (DoS) vulnerability in versions prior to 9.0.2-103. Successful exploitation of this vulnerability on the Cisco ASA-CX could cause the device to stop processing user traffic and prevent management access to the Cisco ASA-CX. Successful exploitation of this vulnerability on the Cisco PRSM could cause the software to become unresponsive and unavailable. There are no workarounds for this vulnerability, but some mitigations are available. Cisco has released free software updates that address this vulnerability.

Cisco Security Advisory 20120912-cupxcp
Cisco Security Advisory - A denial of service (DoS) vulnerability exists in Cisco Unified Presence and Jabber Extensible Communications Platform (Jabber XCP). An unauthenticated, remote attacker could exploit this vulnerability by sending a specially crafted Extensible Messaging and Presence Protocol (XMPP) stream header to an affected server. Successful exploitation of this vulnerability could cause the Connection Manager process to crash. Repeated exploitation could result in a sustained DoS condition. There are no workarounds available to mitigate exploitation of this vulnerability. Cisco has released free software updates that address this vulnerability.

Citrix

Secunia Security Advisory 50536
Secunia Security Advisory - A vulnerability has been reported in Citrix XenApp Online Plug-in and Citrix Receiver, which can be exploited by malicious people to compromise a user's system.

Debian

Debian Security Advisory 2550-1
Debian Linux Security Advisory 2550-1 - Several vulnerabilities were discovered in Asterisk, a PBX and telephony toolkit, allowing privilege escalation in the Asterisk Manager, denial of service or privilege escalation.

Secunia Security Advisory 50583
Secunia Security Advisory - Debian has issued an update for tor. This fixes a vulnerability, which can be exploited by malicious people to cause a DoS (Denial of Service).

Secunia Security Advisory 50560
Secunia Security Advisory - Debian has issued an update for bind9. This fixes a vulnerability, which can be exploited by malicious people to cause a DoS (Denial of Service).

Debian Security Advisory 2549-1
Debian Linux Security Advisory 2549-1 - Multiple vulnerabilities have been discovered in devscripts, a set of scripts to make the life of a Debian Package maintainer easier.

Debian Security Advisory 2480-4
Debian Linux Security Advisory 2480-4 - The security updates for request-tracker3.8, DSA-2480-1, DSA-2480-2, and DSA-2480-3, contained minor regressions.

Debian Security Advisory 2548-1
Debian Linux Security Advisory 2548-1 - Severel vulnerabilities have been discovered in Tor, an online privacy tool.

Debian Security Advisory 2546-1
Debian Linux Security Advisory 2546-1 - Timo Warns discovered that the EAP-TLS handling of freeradius, a high-performance and highly configurable RADIUS server, is not properly performing length checks on user-supplied input before copying to a local stack buffer. As a result, an unauthenticated attacker can exploit this flaw to crash the daemon or execute arbitrary code via crafted certificates.

Debian Security Advisory 2547-1
Debian Linux Security Advisory 2547-1 - It was discovered that BIND, a DNS server, does not handle DNS records properly which approach size limits inherent to the DNS protocol. An attacker could use crafted DNS records to crash the BIND server process, leading to a denial of service.

IBM

IBM Java Security Vulnerabilities
Security Explorations discovered multiple security vulnerabilities in IBM SDK, Java Technology Edition software. This is IBM's implementation of Java SE technology for AIX, Linux, z/OS and IBMi platforms. Among a total of 17 security weaknesses found, there are issues that can lead to the complete compromise of a target IBM Java environment.

Secunia Security Advisory 50619
Secunia Security Advisory - A vulnerability has been reported in IBM AIX, which can be exploited by malicious people to cause a DoS (Denial of Service

Secunia Security Advisory 50607
Secunia Security Advisory - IBM has acknowledged multiple vulnerabilities in IBM Java, which can be exploited by malicious, local users to disclose potentially sensitive data and by malicious people to disclose potentially sensitive information, manipulate certain data, cause a DoS (Denial of Service), and compromise a vulnerable system.

Mandriva

Mandriva Linux Security Advisory 2012-150
Mandriva Linux Security Advisory 2012-150 - Multiple security issues were identified and fixed in OpenJDK (icedtea6). Unspecified vulnerability in the Java Runtime Environment component in Oracle Java SE 7 Update 6 and earlier, and 6 Update 34 and earlier, has no impact and remote attack vectors involving AWT and a security-in-depth issue that is not directly exploitable but which can be used to aggravate security vulnerabilities that can be directly exploited. Unspecified vulnerability in the Java Runtime Environment component in Oracle Java SE 7 Update 6 and earlier allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Beans, a different vulnerability than CVE-2012-3136. The updated packages provides icedtea6-1.11.4 which is not vulnerable to these issues.

Mandriva Linux Security Advisory 2012-151
Mandriva Linux Security Advisory 2012-151 - An integer overflow flaw, leading to a heap-based buffer overflow, was found in Ghostscript's International Color Consortium Format library. An attacker could create a specially-crafted PostScript or PDF file with embedded images that would cause Ghostscript to crash or, potentially, execute arbitrary code with the privileges of the user running Ghostscript. The updated packages have been patched to correct this issue.

Mandriva Linux Security Advisory 2012-153
Mandriva Linux Security Advisory 2012-153 - ISC DHCP 4.1.x before 4.1-ESV-R7 and 4.2.x before 4.2.4-P2 allows remote attackers to cause a denial of service in opportunistic circumstances by establishing an IPv6 lease in an environment where the lease expiration time is later reduced. The updated packages have been patched to correct this issue.

Mandriva Linux Security Advisory 2012-152
Mandriva Linux Security Advisory 2012-152 - A nameserver can be caused to exit with a REQUIRE exception if it can be induced to load a specially crafted resource record. The updated packages have been upgraded to bind 9.7.6-P3 which is not vulnerable to this issue.

Microsoft

Technical Cyber Security Alert 2012-262A
Technical Cyber Security Alert 2012-262A - An unpatched use-after-free vulnerability in Microsoft Internet Explorer versions 7, 8, and 9 is being exploited in the wild. Microsoft has released Security Advisory 2757760 with mitigation techniques.

Microsoft Windows Common Controls MSCOMCTL.OCX Use-After-Free
VUPEN Vulnerability Research Team discovered a critical vulnerability in Microsoft products. The vulnerability is caused by a use-after-free error in the "TabStrip" Control within the "MSCOMCTL.OCX" component, which could allow remote attackers execute arbitrary code via a specially crafted web page or malicious Office document. A large amount of products are affected.

Microsoft Security Bulletin Summary For September 2012
This bulletin summary lists 2 released Microsoft security bulletins for September, 2012.

Technical Cyber Security Alert 2012-255A
Technical Cyber Security Alert 2012-255A - Select Microsoft software products contain multiple vulnerabilities. Microsoft has released updates to address these vulnerabilities.

Mozilla

Mozilla Firefox nsHTMLEditRules Remote Use-After-Free
VUPEN Vulnerability Research Team discovered a critical vulnerability in Mozilla Firefox. The vulnerability is caused by a use-after-free error in the "setUserData()" method within the "nsHTMLEditRules" class, which could allow remote attackers execute arbitrary code via a specially crafted web page. Products affected include Mozilla Firefox versions prior to 15, Mozilla Firefox ESR versions prior to 10.0.7, Mozilla Thunderbird versions prior to 15, Mozilla Thunderbird ESR versions prior to 10.0.7, and Mozilla SeaMonkey versions prior to 2.12.

Secunia Security Advisory 50616
Secunia Security Advisory - SUSE has issued an update for MozillaFirefox. This fixes multiple vulnerabilities, which can be exploited by malicious people to disclose potentially sensitive information, conduct cross-site scripting and phishing attacks, and compromise a user's system.

Novell

Novell GroupWise iCalendar Date/Time Parsing Denial of Service
in Novell GroupWise, which can be exploited by malicious people to cause a DoS (Denial of Service). However, no checks are performed by a function in iCalendar to ensure that the supplied date-time string is longer than 8 characters. This may result in an out-of-bounds read access violation, causing GWIA to crash in case a shorter date-time string was supplied via e.g. an e-mail with a specially crafted .ics attachment. Novell GroupWise version 8.0.2 HP3 is affected.

Secunia Security Advisory 50622
Secunia Security Advisory - Francis Provencher has discovered a vulnerability in Novell GroupWise, which can be exploited by malicious people to potentially compromise a vulnerable system.

Red Hat

Red Hat Security Advisory 2012-1289-01
Red Hat Security Advisory 2012-1289-01 - IBM Java SE version 7 includes the IBM Java Runtime Environment and the IBM Java Software Development Kit. This update fixes several vulnerabilities in the IBM Java Runtime Environment and the IBM Java Software Development Kit.

Secunia Security Advisory 50609
Secunia Security Advisory - Red Hat has issued an update for quagga. This fixes multiple vulnerabilities, which can be exploited by malicious people to cause a DoS (Denial of Service).

Secunia Security Advisory 50624
Secunia Security Advisory - Red Hat has issued an update for quagga. This fixes multiple vulnerabilities, which can be exploited by malicious people to cause a DoS (Denial of Service).

Red Hat Security Advisory 2012-1288-01
Red Hat Security Advisory 2012-1288-01 - The libxml2 library is a development toolbox providing the implementation of various XML standards. Multiple integer overflow flaws, leading to heap-based buffer overflows, were found in the way libxml2 handled documents that enable entity expansion. A remote attacker could provide a large, specially-crafted XML file that, when opened in an application linked against libxml2, would cause the application to crash or, potentially, execute arbitrary code with the privileges of the user running the application. A one byte buffer overflow was found in the way libxml2 evaluated certain parts of XML Pointer Language expressions. A remote attacker could provide a specially-crafted XML file that, when opened in an application linked against libxml2, would cause the application to crash or, potentially, execute arbitrary code with the privileges of the user running the application.

Secunia Security Advisory 50636
Secunia Security Advisory - Red Hat has issued an update for postgresql. This fixes a vulnerability, which can be exploited by malicious people to compromise a user's system.

Secunia Security Advisory 50634
Secunia Security Advisory - Red Hat has issued an update for libxslt. This fixes multiple vulnerabilities, which can be exploited by malicious people to disclose system information, cause a DoS (Denial of Service), and compromise an application using the library.

Secunia Security Advisory 50635
Secunia Security Advisory - Red Hat has issued an update for postgresql and postgresql84. This fixes two vulnerabilities, which can be exploited by malicious people to disclose certain sensitive information and compromise a user's system.

Red Hat Security Advisory 2012-1267-01
Red Hat Security Advisory 2012-1267-01 - The Berkeley Internet Name Domain is an implementation of the Domain Name System protocols. BIND includes a DNS server ; a resolver library ; and tools for verifying that the DNS server is operating correctly. A flaw was found in the way BIND handled resource records with a large RDATA value. A malicious owner of a DNS domain could use this flaw to create specially-crafted DNS resource records, that would cause a recursive resolver or secondary server to exit unexpectedly with an assertion failure.

Red Hat Security Advisory 2012-1268-01
Red Hat Security Advisory 2012-1268-01 - The Berkeley Internet Name Domain is an implementation of the Domain Name System protocols. BIND includes a DNS server ; a resolver library ; and tools for verifying that the DNS server is operating correctly. A flaw was found in the way BIND handled resource records with a large RDATA value. A malicious owner of a DNS domain could use this flaw to create specially-crafted DNS resource records, that would cause a recursive resolver or secondary server to exit unexpectedly with an assertion failure.

Red Hat Security Advisory 2012-1266-01
Red Hat Security Advisory 2012-1266-01 - The Berkeley Internet Name Domain is an implementation of the Domain Name System protocols. BIND includes a DNS server ; a resolver library ; and tools for verifying that the DNS server is operating correctly. A flaw was found in the way BIND handled resource records with a large RDATA value. A malicious owner of a DNS domain could use this flaw to create specially-crafted DNS resource records, that would cause a recursive resolver or secondary server to exit unexpectedly with an assertion failure.

Secunia Security Advisory 50582
Secunia Security Advisory - Red Hat has issued an update for bind97. This fixes a vulnerability, which can be exploited by malicious people to cause a DoS (Denial of Service).

Red Hat Security Advisory 2012-1265-01
Red Hat Security Advisory 2012-1265-01 - libxslt is a library for transforming XML files into other textual formats using the standard XSLT stylesheet transformation mechanism. A heap-based buffer overflow flaw was found in the way libxslt applied templates to nodes selected by certain namespaces. An attacker could use this flaw to create a malicious XSL file that, when used by an application linked against libxslt to perform an XSL transformation, could cause the application to crash or, possibly, execute arbitrary code with the privileges of the user running the application.

Red Hat Security Advisory 2012-1263-01
Red Hat Security Advisory 2012-1263-01 - PostgreSQL is an advanced object-relational database management system. It was found that the optional PostgreSQL xml2 contrib module allowed local files and remote URLs to be read and written to with the privileges of the database server when parsing Extensible Stylesheet Language Transformations. An unprivileged database user could use this flaw to read and write to local files and remote URLs they would otherwise not have access to by issuing a specially-crafted SQL query.

Red Hat Security Advisory 2012-1264-01
Red Hat Security Advisory 2012-1264-01 - PostgreSQL is an advanced object-relational database management system. It was found that the optional PostgreSQL xml2 contrib module allowed local files and remote URLs to be read and written to with the privileges of the database server when parsing Extensible Stylesheet Language Transformations. An unprivileged database user could use this flaw to read and write to local files and remote URLs they would otherwise not have access to by issuing a specially-crafted SQL query.

Red Hat Security Advisory 2012-1261-01
Red Hat Security Advisory 2012-1261-01 - D-Bus is a system for sending messages between applications. It is used for the system-wide message bus service and as a per-user-login-session messaging facility. It was discovered that the D-Bus library honored environment settings even when running with elevated privileges. A local attacker could possibly use this flaw to escalate their privileges, by setting specific environment variables before running a setuid or setgid application linked against the D-Bus library. Note: With this update, libdbus ignores environment variables when used by setuid or setgid applications. The environment is not ignored when an application gains privileges via file system capabilities; however, no application shipped in Red Hat Enterprise Linux 6 gains privileges via file system capabilities.

Red Hat Security Advisory 2012-1262-01
Red Hat Security Advisory 2012-1262-01 - The rhev-hypervisor5 package provides a Red Hat Enterprise Virtualization Hypervisor ISO disk image. The Red Hat Enterprise Virtualization Hypervisor is a dedicated Kernel-based Virtual Machine hypervisor. It includes everything necessary to run and manage virtual machines: A subset of the Red Hat Enterprise Linux operating environment and the Red Hat Enterprise Virtualization Agent. Note: Red Hat Enterprise Virtualization Hypervisor is only available for the Intel 64 and AMD64 architectures with virtualization extensions. A flaw was found in the way QEMU handled VT100 terminal escape sequences when emulating certain character devices. A guest user with privileges to write to a character device that is emulated on the host using a virtual console back-end could use this flaw to crash the qemu-kvm process on the host or, possibly, escalate their privileges on the host.

Secunia Security Advisory 50544
Secunia Security Advisory - Red Hat has issued an update for dbus. This fixes a vulnerability, which can be exploited by malicious, local users to gain escalated privileges.

Secunia Security Advisory 50579
Secunia Security Advisory - Red Hat has issued an update for bind. This fixes a vulnerability, which can be exploited by malicious people to cause a DoS (Denial of Service).

Red Hat Security Advisory 2012-1259-01
Red Hat Security Advisory 2012-1259-01 - Quagga is a TCP/IP based routing software suite. The Quagga bgpd daemon implements the BGP routing protocol. The Quagga ospfd and ospf6d daemons implement the OSPF routing protocol. A heap-based buffer overflow flaw was found in the way the bgpd daemon processed malformed Extended Communities path attributes. An attacker could send a specially-crafted BGP message, causing bgpd on a target system to crash or, possibly, execute arbitrary code with the privileges of the user running bgpd. The UPDATE message would have to arrive from an explicitly configured BGP peer, but could have originated elsewhere in the BGP network.

Red Hat Security Advisory 2012-1258-01
Red Hat Security Advisory 2012-1258-01 - Quagga is a TCP/IP based routing software suite. The Quagga bgpd daemon implements the BGP routing protocol. The Quagga ospfd and ospf6d daemons implement the OSPF routing protocol. A heap-based buffer overflow flaw was found in the way the bgpd daemon processed malformed Extended Communities path attributes. An attacker could send a specially-crafted BGP message, causing bgpd on a target system to crash or, possibly, execute arbitrary code with the privileges of the user running bgpd. The UPDATE message would have to arrive from an explicitly configured BGP peer, but could have originated elsewhere in the BGP network.

Secunia Security Advisory 50587
Secunia Security Advisory - Red Hat has issued an update for libexif. This fixes multiple vulnerabilities, which can be exploited by malicious people to disclose certain sensitive information, cause a DoS (Denial of Service), and compromise an application using the library.

Red Hat Security Advisory 2012-1284-01
Red Hat Security Advisory 2012-1284-01 - The spice-gtk packages provide a GIMP Toolkit widget for SPICE clients. Both Virtual Machine Manager and Virtual Machine Viewer can make use of this widget to access virtual machines using the SPICE protocol. It was discovered that the spice-gtk setuid helper application, spice-client-glib-usb-acl-helper, did not clear the environment variables read by the libraries it uses. A local attacker could possibly use this flaw to escalate their privileges by setting specific environment variables before running the helper application.

Red Hat Security Advisory 2012-1283-01
Red Hat Security Advisory 2012-1283-01 - OpenJPEG is an open source library for reading and writing image files in JPEG 2000 format. It was found that OpenJPEG failed to sanity-check an image header field before using it. A remote attacker could provide a specially-crafted image file that could cause an application linked against OpenJPEG to crash or, possibly, execute arbitrary code. This issue was discovered by Huzaifa Sidhpurwala of the Red Hat Security Response Team.

Red Hat Security Advisory 2012-1255-01
Red Hat Security Advisory 2012-1255-01 - The libexif packages provide an Exchangeable image file format library. Exif allows metadata to be added to and read from certain types of image files. Multiple flaws were found in the way libexif processed Exif tags. An attacker could create a specially-crafted image file that, when opened in an application linked against libexif, could cause the application to crash or, potentially, execute arbitrary code with the privileges of the user running the application.

Red Hat Security Advisory 2012-1256-01
Red Hat Security Advisory 2012-1256-01 - Ghostscript is a set of software that provides a PostScript interpreter, a set of C procedures and an interpreter for Portable Document Format files. An integer overflow flaw, leading to a heap-based buffer overflow, was found in Ghostscript's International Color Consortium Format library. An attacker could create a specially-crafted PostScript or PDF file with embedded images that would cause Ghostscript to crash or, potentially, execute arbitrary code with the privileges of the user running Ghostscript.

RSA

Secunia Security Advisory 50605
Secunia Security Advisory - EMC has acknowledged a weakness in RSA BSAFE, which can be exploited by malicious people to disclose potentially sensitive information and hijack a user's session.

Secunia Security Advisory 50601
Secunia Security Advisory - EMC has acknowledged a weakness and a vulnerability in RSA BSAFE, which can be exploited by malicious people to disclose sensitive information, hijack a user's session, and potentially compromise an application using the library.

RSA BSAFE SSL-C 2.8.6 BEAST / Buffer Overflow Fixes
RSA BSAFE SSL-C version 2.8.6 contains fixes designed to prevent BEAST attacks and buffer overflow vulnerabilities.

RSA BSAFE Micro Edition Suite Security Update for BEAST Attacks
RSA BSAFE Micro Edition Suite contains updates designed to prevent BEAST attacks. There is a known vulnerability in SSLv3 and TLS v1.0 to do with how the Initialization Vector (IV) is generated. For symmetric key algorithms in CBC mode, the IV for the first record is generated using keys and secrets set during the SSL or TLS handshake. All subsequent records are encrypted using the ciphertext block from the previous record as the IV. With symmetric key encryption in CBC mode, plain text encrypted with the same IV and key generates the same cipher text, which is why having a variable IV is important. The BEAST exploit uses this SSLv3 and TLS v1.0 vulnerability by allowing an attacker to observe the last ciphertext block, which is the IV, then replace this with an IV of their choice, inject some of their own plain text data, and when this new IV is used to encrypt the data, the attacker can guess the plain text data one byte at a time.

Slackware

Slackware Security Advisory - patch Updates
Slackware Security Advisory - New patch packages are available for Slackware 12.1, 12.2, 13.0, 13.1, 13.37, and -current to fix a security issue

Slackware Security Advisory - bind Updates
Slackware Security Advisory - New bind packages are available for Slackware 12.1, 12.2, 13.0, 13.1, 13.37, and -current to fix a security issue.

Slackware Security Advisory - dhcp Updates
Slackware Security Advisory - New dhcp packages are available for Slackware 12.1, 12.2, 13.0, 13.1, 13.37, and -current to fix a security issue.

Siemens

Secunia Security Advisory 50630
Secunia Security Advisory - A security issue has been reported in Siemens SIMATIC S7-1200, which can be exploited by malicious people to conduct spoofing attacks.

Suse

Secunia Security Advisory 50537
Secunia Security Advisory - SUSE has issued an update for dbus. This fixes a vulnerability, which can be exploited by malicious, local users to gain escalated privileges.

Secunia Security Advisory 50594
Secunia Security Advisory - SUSE has issued an update for compat-openssl097g. This fixes a vulnerability, which can be exploited by malicious people to potentially compromise an application using the library.

Secunia Security Advisory 50621
Secunia Security Advisory - SUSE has issued an update for kvm. This fixes a vulnerability, which can be exploited by malicious, local users in a guest virtual machine to potentially gain escalated privileges.

Ubuntu

Ubuntu Security Notice USN-1571-1
Ubuntu Security Notice 1571-1 - Glen Eustace discovered that the DHCP server incorrectly handled IPv6 expiration times. A remote attacker could use this issue to cause DHCP to crash, resulting in a denial of service. This issue only affected Ubuntu 11.04, Ubuntu 11.10 and Ubuntu 12.04 LTS. Dan Rosenberg discovered that the DHCP AppArmor profile could be escaped by using environment variables. This update mitigates the issue by sanitizing certain variables in the DHCP shell scripts. Various other issues were also addressed.

Ubuntu Security Notice USN-1573-1
Ubuntu Security Notice 1573-1 - Ben Hutchings reported a flaw in the Linux kernel with some network drivers that support TSO (TCP segment offload). A local or peer user could exploit this flaw to to cause a denial of service. Jay Fenlason and Doug Ledford discovered a bug in the Linux kernel implementation of RDS sockets. A local unprivileged user could potentially use this flaw to read privileged information from the kernel. Various other issues were also addressed.

Ubuntu Security Notice USN-1572-1
Ubuntu Security Notice 1572-1 - Ben Hutchings reported a flaw in the Linux kernel with some network drivers that support TSO (TCP segment offload). A local or peer user could exploit this flaw to to cause a denial of service. Jay Fenlason and Doug Ledford discovered a bug in the Linux kernel implementation of RDS sockets. A local unprivileged user could potentially use this flaw to read privileged information from the kernel. Various other issues were also addressed.

Ubuntu Security Notice USN-1568-1
Ubuntu Security Notice 1568-1 - Ben Hutchings reported a flaw in the Linux kernel with some network drivers that support TSO (TCP segment offload). A local or peer user could exploit this flaw to to cause a denial of service. Jay Fenlason and Doug Ledford discovered a bug in the Linux kernel implementation of RDS sockets. A local unprivileged user could potentially use this flaw to read privileged information from the kernel. Various other issues were also addressed.

Ubuntu Security Notice USN-1567-1
Ubuntu Security Notice 1567-1 - A flaw was found in how the Linux kernel passed the replacement session keyring to a child process. An unprivileged local user could exploit this flaw to cause a denial of service (panic). Ben Hutchings reported a flaw in the Linux kernel with some network drivers that support TSO (TCP segment offload). A local or peer user could exploit this flaw to to cause a denial of service. Jay Fenlason and Doug Ledford discovered a bug in the Linux kernel implementation of RDS sockets. A local unprivileged user could potentially use this flaw to read privileged information from the kernel. Various other issues were also addressed.

Ubuntu Security Notice USN-1565-1
Ubuntu Security Notice 1565-1 - Thomas Biege discovered that the Horizon authentication mechanism did not validate the next parameter. An attacker could use this to construct a link to legitimate OpenStack web dashboard that redirected the user to a malicious website after authentication.

Ubuntu Security Notice USN-1564-1
Ubuntu Security Notice 1564-1 - Dolph Mathews discovered that when roles are granted and revoked to users in Keystone, pre-existing tokens were not updated or invalidated to take the new roles into account. An attacker could use this to continue to access resources that have been revoked.

Ubuntu Security Notice USN-1566-1
Ubuntu Security Notice 1566-1 - It was discovered that Bind incorrectly handled certain specially crafted long resource records. A remote attacker could use this flaw to cause Bind to crash, resulting in a denial of service.

Secunia Security Advisory 50532
Secunia Security Advisory - Ubuntu has issued an update for horizon. This fixes a weakness, which can be exploited by malicious people to conduct spoofing attacks.

Secunia Security Advisory 50590
Secunia Security Advisory - Ubuntu has issued an update for keystone. This fixes a security issue, which can be exploited by malicious users to bypass certain security restrictions.

Secunia Security Advisory 50497
Secunia Security Advisory - A vulnerability has been reported in System Center Configuration Manager, which can be exploited by malicious people to conduct cross-site scripting attacks.

Secunia Security Advisory 50559
Secunia Security Advisory - Ubuntu has issued an update for xmlrpc. This fixes a vulnerability, which can be exploited by malicious people to cause a DoS (Denial of Service) in an application using the library.

Secunia Security Advisory 50563
Secunia Security Advisory - Ubuntu has issued an update for ubiquity-slideshow-ubuntu. This fixes a a weakness, which can be exploited by malicious people to conduct spoofing attacks.

Secunia Security Advisory 50567
Secunia Security Advisory - Ubuntu has issued an update for python-django. This fixes two security issues and a vulnerability, which can be exploited by malicious people to conduct cross-site scripting attacks and cause a DoS (Denial of Service).

Secunia Security Advisory 50650
Secunia Security Advisory - Ubuntu has issued an update for the kernel. This fixes some vulnerabilities, which can be exploited by malicious, local users and malicious people to cause a DoS (Denial of Service).

Ubuntu Security Notice USN-1570-1
Ubuntu Security Notice 1570-1 - It was discovered that GnuPG used a short ID when downloading keys from a keyserver, even if a long ID was requested. An attacker could possibly use this to return a different key with a duplicate short key id.

Ubuntu Security Notice USN-1548-2
Ubuntu Security Notice 1548-2 - USN-1548-1 fixed vulnerabilities in Firefox. The new package caused a regression in Private Browsing which could leak sites visited to the browser cache. This update fixes the problem. Gary Kwong, Christian Holler, Jesse Ruderman, Steve Fink, Bob Clary, Andrew Sutherland, Jason Smith, John Schoenick, Vladimir Vukicevic and Daniel Holbert discovered memory safety issues affecting Firefox. If the user were tricked into opening a specially crafted page, an attacker could possibly exploit these to cause a denial of service via application crash, or potentially execute code with the privileges of the user invoking Firefox. Abhishek Arya discovered multiple use-after-free vulnerabilities. If the user were tricked into opening a specially crafted page, an attacker could exploit these to cause a denial of service via application crash, or potentially execute code with the privileges of the user invoking Firefox. Various other issues were also addressed.

Ubuntu Security Notice USN-1569-1
Ubuntu Security Notice 1569-1 - It was discovered that PHP incorrectly handled certain character sequences when applying HTTP response-splitting protection. A remote attacker could create a specially-crafted URL and inject arbitrary headers. It was discovered that PHP incorrectly handled directories with a large number of files. This could allow a remote attacker to execute arbitrary code with the privileges of the web server, or to perform a denial of service. Various other issues were also addressed.

Ubuntu Security Notice USN-1563-1
Ubuntu Security Notice 1563-1 - A flaw was found in the Linux kernel's Reliable Datagram Sockets (RDS) protocol implementation. A local, unprivileged user could use this flaw to cause a denial of service.

Ubuntu Security Notice USN-1562-1
Ubuntu Security Notice 1562-1 - Some errors where discovered in the Linux kernel's UDF file system, which is used to mount some CD-ROMs and DVDs. An unprivileged local user could use these flaws to crash the system.

Ubuntu Security Notice USN-1527-2
Ubuntu Security Notice 1527-2 - USN-1527-1 fixed vulnerabilities in Expat. This update provides the corresponding updates for XML-RPC for C and C++. Both issues described in the original advisory affected XML-RPC for C and C++ in Ubuntu 10.04 LTS, 11.04, 11.10 and 12.04 LTS. It was discovered that Expat computed hash values without restricting the ability to trigger hash collisions predictably. If a user or application linked against Expat were tricked into opening a crafted XML file, an attacker could cause a denial of service by consuming excessive CPU resources. Tim Boddy discovered that Expat did not properly handle memory reallocation when processing XML files. If a user or application linked against Expat were tricked into opening a crafted XML file, an attacker could cause a denial of service by consuming excessive memory resources. This issue only affected Ubuntu 8.04 LTS, 10.04 LTS, 11.04 and 11.10. Various other issues were also addressed.

Misc:
Secunia Security Advisory 50527
Secunia Security Advisory - A security issue has been reported in Vino, which can be exploited by malicious people to disclose certain sensitive information.

Secunia Security Advisory 50641
Secunia Security Advisory – A vulnerability has been reported in eZ Publish, which can be exploited by malicious people to conduct script insertion attacks.

Secunia Security Advisory 50598
Secunia Security Advisory - A vulnerability has been discovered in OpenX, which can be exploited by malicious people to conduct SQL injection attacks.

Secunia Security Advisory 50610
Secunia Security Advisory - A vulnerability has been reported in ISC BIND, which can be exploited by malicious people to cause a DoS (Denial of Service).

Secunia Security Advisory 50546
Secunia Security Advisory - A vulnerability has been reported in the Mass Contact module for Drupal, which can be exploited by malicious users to bypass certain security restrictions.

Secunia Security Advisory 50612
Secunia Security Advisory - A security issue has been reported in ISC DHCP, which can be exploited by malicious people to cause a DoS (Denial of Service).

Secunia Security Advisory 50534
Secunia Security Advisory - A vulnerability has been reported in the PDFThumb module for Drupal, which can be exploited by malicious users to compromise a vulnerable system.

Secunia Security Advisory 50557
Secunia Security Advisory - A vulnerability has been reported in the Inf08 theme for Drupal, which can be exploited by malicious users to conduct script insertion attacks.

Secunia Security Advisory 50569
Secunia Security Advisory - A vulnerability has been reported in Pomm, which can be exploited by malicious people to conduct SQL injection attacks.

Secunia Security Advisory 50531
Secunia Security Advisory - A security issue has been reported in OpenStack Keystone, which can be exploited by malicious users to bypass certain security restrictions.

Secunia Security Advisory 50130
Secunia Security Advisory - Georgi Geshev has discovered a vulnerability in OpenSLP, which can be exploited by malicious people to cause a DoS (Denial of Service).

Secunia Security Advisory 50535
Secunia Security Advisory - A security issue has been reported in Bacula, which can be exploited by malicious users to bypass certain security restrictions.

Secunia Security Advisory 50589
Secunia Security Advisory - A vulnerability has been reported in Smarty, which can be exploited by malicious people to conduct cross-site scripting attacks.

Secunia Security Advisory 50529
Secunia Security Advisory - A vulnerability has been reported in Python trytond Module, which can be exploited by malicious users to bypass certain security restrictions.

Secunia Security Advisory 50558
Secunia Security Advisory - A security issue has been discovered in Akcms, which can be exploited by malicious people to disclose sensitive information.

Secunia Security Advisory 50593
Secunia Security Advisory - McAfee has acknowledged multiple vulnerabilities in McAfee Firewall Enterprise, which can be exploited by malicious people to cause a DoS (Denial of Service).

Secunia Security Advisory 50644
Secunia Security Advisory - Some vulnerabilities have been reported in Eucalyptus, which can be exploited by malicious users to bypass certain security restrictions and cause a DoS (Denial of Service).

Secunia Security Advisory 50617
Secunia Security Advisory - Multiple vulnerabilities have been discovered in Auxilium PetRatePro, which can be exploited by malicious people to conduct cross-site request and SQL injection attacks and compromise a vulnerable system.

Secunia Security Advisory 50539
Secunia Security Advisory - High-Tech Bridge has discovered multiple vulnerabilities in TCExam, which can be exploited by malicious users to conduct SQL injection attacks and by malicious people to conduct cross-site scripting attacks.

Secunia Security Advisory 50584
Secunia Security Advisory - Debian has issued an update for freeradius. This fixes a vulnerability, which can be exploited by malicious people to compromise a vulnerable system.

Secunia Security Advisory 50606
Secunia Security Advisory - A vulnerability has been reported in Atlassian Confluence, which can be exploited by malicious people to conduct cross-site scripting attacks.

Secunia Security Advisory 50523
Secunia Security Advisory - A vulnerability has been reported in ColdFusion, which can be exploited by malicious people to cause a DoS (Denial of Service).

Secunia Security Advisory 50511
Secunia Security Advisory - Reaction Information Security has discovered a vulnerability in the Download Monitor plugin for WordPress, which can be exploited by malicious people to conduct cross-site scripting attacks.

Secunia Security Advisory 50463
Secunia Security Advisory - A vulnerability has been reported in Visual Studio Team Foundation Server, which can be exploited by malicious people to conduct cross-site scripting attacks.

Secunia Security Advisory 50564
Secunia Security Advisory - Ubuntu has issued an update for gimp. This fixes two vulnerabilities, which can be exploited by malicious people to compromise a user's system.

Secunia Security Advisory 50561
Secunia Security Advisory - A vulnerability has been reported in F5 BIG-IP ASM, which can be exploited by malicious people to conduct cross-site scripting attacks.

Secunia Security Advisory 50508
Secunia Security Advisory - Certezz has reported a security issue in DTE Axiom, which can be exploited by malicious users to bypass certain security restrictions.

Secunia Security Advisory 50568
Secunia Security Advisory - Multiple vulnerabilities have been reported in Siemens SIMATIC WinCC, which can be exploited by malicious people to conduct cross-site scripting attacks, conduct SQL injection attacks, and disclose certain sensitive information.

Secunia Security Advisory 50484
Secunia Security Advisory - A vulnerability has been reported in FreeRADIUS, which can be exploited by malicious people to compromise a vulnerable system.

Secunia Security Advisory 50581
Secunia Security Advisory - A vulnerability has been reported in Siemens SIMATIC WinCC, which can be exploited by malicious people to conduct cross-site request forgery attacks.

Secunia Security Advisory 50518
Secunia Security Advisory - Two vulnerabilities have been discovered in ViciDial Asterisk GUI Client, which can be exploited by malicious people to conduct cross-site scripting attacks.

Secunia Security Advisory 50599
Secunia Security Advisory - loneferret has discovered a vulnerability in qdPM, which can be exploited by malicious users to compromise a vulnerable system

Secunia Security Advisory 50578
Secunia Security Advisory - Two vulnerabilities have been reported in Tor, which can be exploited by malicious people to cause a DoS (Denial of Service).

Tools released this week:

UK CPNI IPv6 Toolkit 1.2.3
This toolkit houses various IPv6 tools that have been tested to compile and run on Debian GNU/Linux 6.0, FreeBSD 9.0, NetBSD 5.1, OpenBSD 5.0, Mac OS 10.8.0, and Ubuntu 11.10.
Changes: Various updates and OSes supported.

IPv6 Address Monitoring Tool 1.0
ipv6mon is a tool for monitoring IPv6 address usage on a local network. It is meant to be particularly useful in networks that employ IPv6 Stateless Address Auto-Configuration (as opposed to DHCPv6), where address assignment is decentralized and there is no central server that records which IPv6 addresses have been assigned to which nodes during which period of time. ipv6mon employs active probing to discover IPv6 addresses in use, and determine whether such addresses remain active. Changes: Various updates.

360-FAAR Firewall Analysis Audit And Repair 0.2.9
360-FAAR Firewall Analysis Audit and Repair is an offline command line perl policy manipulation tool to filter, compare to logs, merge, translate and output firewall commands for new policies, in checkpoint dbedit or screenos commands. Changes: This release further upgrades the NAT analysis capabilities, more NAT details are listed in 'print' mode.

Skipfish Web Application Scanner 2.09b
Skipfish is a fully automated, active web application security reconnaissance tool. It is high speed, has a low false positive rate, and is easy to use. Changes: Fixed a crash that could be triggered during 404 fingerprint failures. Signature IDs for detected issues are now stored in the report JSON files. Added mod_status, mod_info, MySQL dump, phpMyAdmin SQL dump and robots.txt signatures. Improve

TOR Virtual Network Tunneling Tool 0.2.2.39
Tor is a network of virtual tunnels that allows people and groups to improve their privacy and security on the Internet. It also enables software developers to create new communication tools with built-in privacy features. It provides the foundation for a range of applications that allow organizations and individuals to share information over public networks without compromising their privacy. Individuals can use it to keep remote Websites from tracking them and their family members. They can also use it to connect to resources such as news sites or instant messaging services that are blocked by their local Internet service providers (ISPs).
Changes: This release fixes two opportunities for remotely-triggerable assertions.

WordPress Attack Scanner Free
WordPress Attack Scanner is a plugin for WordPress that acts as a logging utility detecting attacks on a blog

Exploits released this week:

ActiveFax (ActFax) 4.3 Client Importer Buffer Overflow
Apis Design SQL Injection
Auxilium PetRatePro SQL Injection / Shell Upload
Axis VoIP Manager 2.1.5.7 Cross Site Scripting
eking CMS Shell Upload
Fortigate UTM WAF Appliance Cross Site Scripting
Huawei Internet Mobile Overflow
Internet Download Manager All Versions SEH Based Buffer Overflow
Internet Download Manager All Versions Stack Based Buffer Overflow
Internet Download Manager Buffer Overflow
Internet Download Manager SEH Based Buffer Overflow
libdbus 'DBUS_SYSTEM_BUS_ADDRESS' Local Privilege Escalation
Linux udev Netlink Local Privilege Escalation
LuxCal 2.7.0 XSS / LFI / Information Disclosure
MachForm Remote Shell Upload
Mambo / Joomla FCKEditor Local File Inclusion
Microsoft Internet Explorer execCommand Use-After-Free
NCMedia Sound Editor Pro 7.5.1 Buffer Overflow
NCMedia Sound Editor Pro 7.5.1 Buffer Overflow
NCMedia Sound Editor Pro v7.5.1 MRUList201202.dat File Handling Buffer Overflow
Novell Groupwise 8.0.2 HP3 / 2012 Integer Overflow
Openfiler 2.x NetworkCard Command Execution
Openfiler v2.x NetworkCard Command Execution
Oracle BTM FlashTunnelService Remote Code Execution
Sitecom MD-25x Multiple Vulnerabilities Reverse Root Shell Exploit
Sitecom MD-25x Reverse Root Shell
SonicWALL EMail Security 7.3.5 Cross Site Scripting
Symantec Messaging Gateway 9.5/9.5.1 SSH Default Password Security Bypass Vulnerability
TorrentTrader 2.08 XSS / Directory Traversal / Bypass
WAN Emulator 2.3 Command Execution
WAN Emulator v2.3 Command Execution
Webmin /file/show.cgi Remote Command Execution
Winamp MAKI Buffer Overflow
Winamp MAKI Buffer Overflow

DoS attacks:

Novell Groupwise 8.0.2 HP3 and 2012 Integer Overflow Vulnerability
Oracle VM VirtualBox 4.1 Local Denial of Service Vulnerability
WAP Proof 2008 Denial of Service

Shellcode:

[Raspberry Pi] Linux/ARM - reverse_shell(tcp,10.1.1.2,0x1337)
[Raspberry Pi] Linux/ARM - chmod("/etc/shadow", 0777) - 41 bytes
[Raspberry Pi] Linux/ARM - execve("/bin/sh", [0], [0 vars]) - 30 bytes

Website attacks:

AsaanCart 0.9 Cross Site Scripting
ANTEMENE SQL Injection
ASTPP VoIP Billing (4cf207a) Cross Site Scripting
Centersite SQL Injection
CMS United SQL Injection
CNN.com Cross Site Scripting
Confluence Wiki 4.1.4 Cross Site Scripting
Digital Age SQL Injection
Dynamics Of Design SQL Injection
Ezylog Photovoltaic Management SQL Injection
FBDj Stats SQL Injection
Fortigate UTM WAF Appliance Cross Site Scripting
FreeWebshop 2.2.9 Cross Site Scripting / SQL Inj
Harvard Cross Site Scripting
Identity.net.au SQL Injection
IFOBS Cross Site Scripting / Brute Force
LinkedIn Clickjacking / Open Redirection
MediaLab SQL Injection
Megabirlik Bilgi Islem Cross Site Scripting
Minimal Gallery 0.8.1 Cross Site Scripting
NeoBill CMS 0.8 Alpha Cross Site Scripting
Netsweeper WebAdmin Portal CSRF / XSS / SQL Inj
qdPM 7 Arbitrary PHP File Upload
S&S Computer Imaging SQL Injection
SiteGo Remote File Inclusion
Spiceworks 6.0.00993 Cross Site Scripting
Subrion CMS 2.2.1 Cross Site Request Forgery
Subrion CMS 2.2.1 Cross Site Scripting
Trainor SQL Injection
Trend Micro InterScan Messaging Security Suite XSS / CSRF
TWE CMS SQL Injection
University Of Wisconsin - Madison Cross Site Scripting
Vetor Design SQL Injection
Web Biz India SQL Injection
webERP 4.08.4 SQL Injection
Webify Blog Arbitrary File Deletion
Webify Business Directory Arbitrary File Deletion
Webify eDownloads Cart Arbitrary File Deletion
Webify Photo Gallery Arbitrary File Deletion
Wordpress Download Monitor 3.3.5.7 XSS
WordPress Krea3AllMedias SQL Injection
WordPress Tierra Audio Path Disclosure
XRIX SQL Injection

Websites vulnerable to Cross Site Scripting:

Author	Domain	F	Category	Mirror
flexxpoint	bg.888.com	✓	XSS	mirror
Xylitol	recherche-v2.edf.com	✓	XSS	mirror
flexxpoint	www.chevron.com	✗	XSS	mirror
Fabian Cuchietti	www.mercadolibre.cl	✗	XSS	mirror
Fabian Cuchietti	www.mercadolivre.com.pt	✗	XSS	mirror
Fabian Cuchietti	www.mercadolivre.pt	✗	XSS	mirror

Websites Defaced:

Notifier	L	Domain	OS	View
1923Turk		crslegal.gov.ng/index.htm	Win 2003	mirror
1o1or1not1		www.nimc.gov.bd	Linux	mirror
3CUH4CK		bomberospelileo.gob.ec	Linux	mirror
3n_byt3		kemhubri.dephub.go.id/hubla/in...	Linux	mirror
3n_byt3		tka-online.depnakertrans.go.id...	Win 2008	mirror
3n_byt3		www.dgzf.rz.gov.cn/peler.htm	Win 2003	mirror
3n_byt3		baomi.rz.gov.cn/peler.htm	Win 2003	mirror
3n_byt3		www.rzql.rz.gov.cn/peler.htm	Win 2003	mirror
3n_byt3		www.rzsport.gov.cn/peler.htm	Win 2003	mirror
3n_byt3		www.rzmzj.gov.cn/peler.htm	Win 2003	mirror
3n_byt3		www.rzfao.gov.cn/peler.htm	Win 2003	mirror
3n_byt3		www.rzdrc.gov.cn/peler.htm	Win 2003	mirror
3n_byt3		www.rzccad.gov.cn/peler.htm	Win 2003	mirror
3n_byt3		www.dgrk.gov.cn/peler.htm	Win 2003	mirror
3n_byt3		djfw.tjhexi.gov.cn/peler.htm	Win 2003	mirror
3n_byt3		hxcl.tjhexi.gov.cn/peler.htm	Win 2003	mirror
3n_byt3		www.tiantajie.gov.cn/peler.htm	Win 2003	mirror
593 Crew		nuevosistemadejusticiapenalhgo...	Win 2008	mirror
Ali_D3C0D3R		intranet.comune.sanmauriziocan...	Win 2000	mirror
Anarchy Cr3w		gumushaneafad.gov.tr	Win 2008	mirror
ArTiN		www.carlospellegrini.gov.ar//t...	Linux	mirror
ArTiN		www.nusaybin.gov.tr	Linux	mirror
asad hemati		greenbaywi.gov	Linux	mirror
Ashiyane Digital Security Team		www.thakhunram.go.th/web/index...	Linux	mirror
Ashiyane Digital Security Team		www.nmvb.ca.gov	Win 2008	mirror
Ashiyane Digital Security Team		hrnesm.kyzq.gov.cn/hoss.htm	Win 2003	mirror
Ashiyane Digital Security Team		xjmsm.kyzq.gov.cn/hoss.htm	Win 2003	mirror
Ashiyane Digital Security Team		www.banprang.go.th/banprang/fi...	Linux	mirror
Ashiyane Digital Security Team		www.bang-pha.go.th/bangpa/file...	Linux	mirror
Ashiyane Digital Security Team		www.nikhompattana.go.th/home.php	Linux	mirror
Ashiyane Digital Security Team		auditing-school.cad.go.th/ango...	Win 2003	mirror
Ashiyane Digital Security Team		angthong.cad.go.th/angola.html	Win 2003	mirror
Ashiyane Digital Security Team		www.cad.go.th/ewtadmin/angola....	Win 2003	mirror
Ashiyane Digital Security Team		www.mpdah.gov.in/images/scene/...	Win 2003	mirror
Ashiyane Digital Security Team		www.wlcbsl.gov.cn/water.php	Win 2003	mirror
Ashiyane Digital Security Team		www.comune.amelia.tr.it/primoP...	Linux	mirror
Ashiyane Digital Security Team		pakordum.go.th/footter.html	Linux	mirror
Ashiyane Digital Security Team		www.fscoop.gov.cn/hoss.htm	Win 2003	mirror
Audisoft Hacker Team		www.mef.gob.pe/contenidos/serv...	Linux	mirror
BANGLADESH CYBER ARMY		hospitaltomasuribe.gov.co/tpu....	Linux	mirror
Bangladesh Cyber Army		muniarapa.gob.pe/rexo.html	Linux	mirror
Bangladesh Cyber Army		munihuacho.gob.pe/rexo.html	Linux	mirror
Bangladesh Cyber Army		melchor-ocampo.gob.mx/rexo.html	Linux	mirror
Bangladesh Cyber Army		munitirapata.gob.pe/rexo.html	Linux	mirror

Bangladesh Cyber Army	redsaludhuanuco.gob.pe/rexo.html	Linux	mirror
Bangladesh Cyber Army	sbpiura.gob.pe/BCA.html	Linux	mirror
Bangladesh Cyber Army	asipatnacircle.gov.in	Linux	mirror
Barbaros-DZ	www.sipdt.gov.cn	Win 2003	mirror
Barbaros-DZ	www.lzgt.gov.cn	Linux	mirror
Barbaros-DZ	yundou.sqds.gov.cn	Win 2008	mirror
Barbaros-DZ	www.dp-banjiudian.gov.cn	Win 2003	mirror
Barbaros-DZ	www.jrsjj.gov.cn/dz.htm	Win 2003	mirror
Barbaros-DZ	lhzx.pljy.gov.cn	Win 2003	mirror
Barbaros-DZ	hc.gssn.gov.cn	Win 2008	mirror
Barbaros-DZ	mail.yqtjj.gov.cn	Win 2003	mirror
Barbaros-DZ	xw.fangcheng.gov.cn	Win 2003	mirror
Barbaros-DZ	wx.xncx.gov.cn	Win 2003	mirror
Barbaros-DZ	www.scspfy.gov.cn	Win 2003	mirror
Barbaros-DZ	www.xssfj.gov.cn	Win 2003	mirror
Barbaros-DZ	www.tcmz.gov.cn	Win 2003	mirror
Barbaros-DZ	fy.ycwhj.gov.cn	Win 2003	mirror
Barbaros-DZ	dj.xinhuang.gov.cn	Win 2008	mirror
Barbaros-DZ	fl.tx.gov.cn	Win 2003	mirror
Barbaros-DZ	dangshi.weicheng.gov.cn/dz.htm	Win 2003	mirror
Barbaros-DZ	www.bblzh.gov.cn	Win 2003	mirror
Barbaros-DZ	lzmz.luzhou.gov.cn	Win 2003	mirror
Barbaros-DZ	rhtsg.hengdong.gov.cn	Win 2003	mirror
Barbaros-DZ	www.bdhhb.gov.cn	Win 2003	mirror
Barbaros-DZ	www.stats-hbsz.gov.cn	Win 2003	mirror
Barbaros-DZ	sytj.shiyan.gov.cn	Win 2003	mirror
Barbaros-DZ	www.whfdaxz.gov.cn	Win 2003	mirror
BMPoC	www.unesco.lacult.org/noticias...	Linux	mirror
BOLIVIAN - HACKING	www.beni.gob.bo//manager/data/...	Linux	mirror
BrazilObscure	www.labohidro.ufma.br	Linux	mirror
BrazilObscure	cm-camacari.jusbrasil.com.br/p...	Linux	mirror
c4	www.jppkk.gov.my/esis2/perpind...	Win 2003	mirror
chinahacker	www.finance-mof.gov.cn/dhthack...	Win 2008	mirror
Climax	www.liceomarconi.gov.it	Linux	mirror
ColombianH	www.ramajudicialdelhuila.gov.co	Linux	mirror
Crack999	www.pa-bengkulukota.go.id	Linux	mirror
CrAzY HaCkEr	arsdirectory.regione.liguria.it	Linux	mirror
CrAzY HaCkEr	investimenti.regione.liguria.it	Linux	mirror
CrAzY HaCkEr	www.amicus-partner.regione.lig...	Linux	mirror
CrAzY HaCkEr	www.digitaleterrestre.regione....	Linux	mirror
CrAzY HaCkEr	www.infrastrutture.regione.lig...	Linux	mirror
CrAzY HaCkEr	www.pariopportunita.regione.li...	Linux	mirror
CrAzY HaCkEr	www.ricercasanitaria.regione.l...	Linux	mirror
CrAzY HaCkEr	www.amicus.regione.liguria.it	Linux	mirror
Cyb3rSec	transparencia.bandesal.gob.sv/...	Linux	mirror
Cyb3rSec	formulario.bandesal.gob.sv/s.txt	Linux	mirror
Cyb3rSec	www.munifitzcarraldancash.gob....	Linux	mirror
Cyb3rsec	site.airc.go.ke/images/s.txt	Unknown	mirror

Cybercrookz	mail.perlislib.gov.my/indexx.html	Unknown	mirror
Cyberhackerteam	www.plaengyao.go.th	Win 2003	mirror
Cyberhackerteam	www.pjrkjsw.gov.cn/jsw.php?cla...	Win 2000	mirror
cybertaziex	corregodanta.mg.gov.br	Linux	mirror
cybertaziex	camaramunicipaldeluz.mg.gov.br	Linux	mirror
cybertaziex	quartelgeral.mg.gov.br	Linux	mirror
cybertaziex	camararioparanaiba.mg.gov.br	Linux	mirror
cybertaziex	serradasaudade.mg.gov.br	Linux	mirror
cybertaziex	saaelp.mg.gov.br	Linux	mirror
cybertaziex	ibadannorth.gov.ng	Linux	mirror
DaiLexX	www.embaparusa.gov.py/v1/	Linux	mirror
Dbuzz	sultengprov.go.id	Linux	mirror
Dbuzz	baritotimurkab.go.id/id.htm	Linux	mirror
Dbuzz	www.drsrs.go.ke	Linux	mirror
Dbuzz	www.alsobocaroni.gob.ve/sindic...	Linux	mirror
DevilzSec	stars.mpkj.gov.my/iresponz/Dz.htm	Linux	mirror
DevilzSec	www.blpk.gov.my/esis2/perpinda...	Win 2003	mirror
DevilzSec	tjj.sqsc.gov.cn/index.htm	Win 2003	mirror
DevilzSec	adu-mps.selangor.gov.my/irespo...	Linux	mirror
Digital Boys Underground Team	www.stanford.org/group/swib/cg...	Linux	mirror
Dr-TaiGaR	2011.web.dikti.go.id/stats	Linux	mirror
Dr-TaiGaR	korem051-wkt.mil.id	Linux	mirror
Dr-TaiGaR	www.esantar.furg.br	Linux	mirror
Dr-TaiGaR	www.esantarantartico.furg.br	Linux	mirror
Dr-TaiGaR	www.esantarfrota.furg.br	Linux	mirror
Dr-TaiGaR	www.eteq.furg.br	Linux	mirror
Dr-TaiGaR	www.eticapublica.furg.br	Linux	mirror
Dr-TaiGaR	www.faiq.furg.br	Linux	mirror
Dr-TaiGaR	www.fontes.furg.br	Linux	mirror
Dr-TaiGaR	www.geiam.furg.br	Linux	mirror
Dr-TaiGaR	www.gpciteg.furg.br	Linux	mirror
Dr-TaiGaR	www.hospedagem.furg.br	Linux	mirror
Dr-TaiGaR	www.iceac.furg.br	Linux	mirror
Dr-TaiGaR	www.inctmar.furg.br	Linux	mirror
Dr-TaiGaR	www.io.furg.br	Linux	mirror
Dr-TaiGaR	www.iriorodrigues.furg.br	Linux	mirror
Dr-TaiGaR	www.lacom.furg.br	Linux	mirror
Dr-TaiGaR	www.ladcis.furg.br	Linux	mirror
Dr-TaiGaR	www.lahis.furg.br	Linux	mirror
Dr-TaiGaR	www.lapea.furg.br	Linux	mirror
Dr-TaiGaR	www.lappi.furg.br	Linux	mirror
Dr-TaiGaR	www.lapsicot.furg.br	Linux	mirror
Dr-TaiGaR	www.lca.furg.br	Linux	mirror
Dr-TaiGaR	www.lcsi.furg.br	Linux	mirror
Dr-TaiGaR	www.leme.furg.br	Linux	mirror
Dr-TaiGaR	www.leoc.furg.br	Linux	mirror
Dr-TaiGaR	www.lepd.furg.br	Linux	mirror
Dr-TaiGaR	www.letras.furg.br	Linux	mirror

Dr-TaiGaR	www.lkso.furg.br	Linux	mirror
Dr-TaiGaR	www.lou.furg.br	Linux	mirror
Dr-TaiGaR	www.medicina.furg.br	Linux	mirror
Dr-TaiGaR	www.memoriainfo.furg.br	Linux	mirror
Dr-TaiGaR	www.memoriainvitro.furg.br	Linux	mirror
Dr-TaiGaR	www.modelagemcomputacional.fur...	Linux	mirror
Dr-TaiGaR	www.muvie.furg.br	Linux	mirror
Dr-TaiGaR	www.nac.furg.br	Linux	mirror
Dr-TaiGaR	www.nacinstrumental.furg.br	Linux	mirror
Dr-TaiGaR	www.nau.furg.br	Linux	mirror
Dr-TaiGaR	www.neai.furg.br	Linux	mirror
Dr-TaiGaR	www.nehisp.furg.br	Linux	mirror
Dr-TaiGaR	www.nelp.furg.br	Linux	mirror
Dr-TaiGaR	www.nepe.furg.br	Linux	mirror
Dr-TaiGaR	www.novostalentosfisica.furg.br	Linux	mirror
Dr-TaiGaR	www.nti.furg.br	Linux	mirror
Dr-TaiGaR	www.nudese.furg.br	Linux	mirror
Dr-TaiGaR	www.numeb.furg.br	Linux	mirror
Dr-TaiGaR	www.nupecof.furg.br	Linux	mirror
Dr-TaiGaR	www.omrg.furg.br	Linux	mirror
Dr-TaiGaR	www.paideia.furg.br	Linux	mirror
Dr-TaiGaR	www.pedagogia.furg.br	Linux	mirror
Dr-TaiGaR	www.pet.furg.br	Linux	mirror
Dr-TaiGaR	www.petalimentos.furg.br	Linux	mirror
Dr-TaiGaR	www.petsabest.furg.br	Linux	mirror
Dr-TaiGaR	www.petsap.furg.br	Linux	mirror
Dr-TaiGaR	www.pgfisica.furg.br	Linux	mirror
Dr-TaiGaR	www.pibid.furg.br	Linux	mirror
Dr-TaiGaR	www.pmdd.furg.br	Linux	mirror
Dr-TaiGaR	www.poshistoria.furg.br	Linux	mirror
Dr-TaiGaR	www.ppgedu.furg.br	Linux	mirror
Dr-TaiGaR	www.ppgenf.furg.br	Linux	mirror
Dr-TaiGaR	www.profocap.furg.br	Linux	mirror
Dr-TaiGaR	www.proinfra.furg.br	Linux	mirror
Dr-TaiGaR	www.promic.furg.br	Linux	mirror
Dr-TaiGaR	www.proplad.furg.br	Linux	mirror
Dr-TaiGaR	www.reuni.furg.br	Linux	mirror
Dr-TaiGaR	www.ruasdoriogrande.furg.br	Linux	mirror
Dr-TaiGaR	www.saeqa.furg.br	Linux	mirror
Dr-TaiGaR	www.saga.furg.br	Linux	mirror
Dr-TaiGaR	www.saj.furg.br	Linux	mirror
Dr-TaiGaR	www.saopelotas.furg.br	Linux	mirror
Dr-TaiGaR	www.sap.furg.br	Linux	mirror
Dr-TaiGaR	www.searqrs.furg.br	Linux	mirror
Dr-TaiGaR	www.sebio.furg.br	Linux	mirror
Dr-TaiGaR	www.secom.furg.br	Linux	mirror
Dr-TaiGaR	www.biblioteca.furg.br	Linux	mirror
Dr-TaiGaR	www.autoficcao.furg.br	Linux	mirror

Dr-TaiGaR	www.artes.furg.br	Linux	mirror
Dr-TaiGaR	www.arquivologia.furg.br	Linux	mirror
Dr-TaiGaR	www.arquivo.furg.br	Linux	mirror
Dr-TaiGaR	www.aquapatos.furg.br	Linux	mirror
Dr-TaiGaR	www.amazoniaazul.furg.br	Linux	mirror
Dr-TaiGaR	www.ceema.furg.br	Linux	mirror
Dr-TaiGaR	ceamecim.furg.br	Linux	mirror
Dr-TaiGaR	bluegroups.furg.br	Linux	mirror
Dr-TaiGaR	goal.furg.br	Linux	mirror
Dr-TaiGaR	www.adm.furg.br	Linux	mirror
Dr-TaiGaR	www.sead.furg.br	Linux	mirror
Dr-TaiGaR	www.ppgquimica.furg.br	Linux	mirror
Dr-TaiGaR	www.aquicultura.furg.br	Linux	mirror
Dr-TaiGaR	www.pdi.furg.br	Linux	mirror
Dr-TaiGaR	www.petenfermagem.furg.br	Linux	mirror
Dr-TaiGaR	www.imef.furg.br	Linux	mirror
Dr-TaiGaR	venetinelmondo.regione.veneto.it	Linux	mirror
Dr-TaiGaR	ead-tec.furg.br	Linux	mirror
Dr-TaiGaR	www.por.regione.puglia.it	Linux	mirror
Dr-TaiGaR	www.sema.furg.br	Linux	mirror
Dr-TaiGaR	www.senallp.furg.br	Linux	mirror
Dr-TaiGaR	www.sexualidadeescola.furg.br	Linux	mirror
Dr-TaiGaR	www.siepetur.furg.br	Linux	mirror
Dr-TaiGaR	www.sintec.furg.br	Linux	mirror
Dr-TaiGaR	www.slamtb.furg.br	Linux	mirror
Dr-TaiGaR	www.teias.furg.br	Linux	mirror
DZ-QTH	blog.wwf.ca	Linux	mirror
DZ-QTH	blog.wwf.eu	Linux	mirror
DZ-QTH	blogs.panda.org	Linux	mirror
DZ-QTH	ecoguru.panda.org	Linux	mirror
DZ-QTH	featurette.panda.org	Linux	mirror
DZ-QTH	mobile.panda.org	Linux	mirror
DZ-QTH	posters.panda.org	Linux	mirror
DZ-QTH	speciestracker.panda.org	Linux	mirror
Dz-Secur	mariajuana.gob.ar	Linux	mirror
ĎЯ.MĦ$ŤĚř ĦåĶ	joinnavy.mil.bd	Linux	mirror
Eg-R1z	youropinion.gov.sy	Win 2008	mirror
Eg-R1z	sytrol.gov.sy	Win 2008	mirror
Fatal Error	www.dadj.uff.br	Linux	mirror
Fatal Error	fil.fafich.ufmg.br	Linux	mirror
Fatal Error	www2.iat.educacao.ba.gov.br	Linux	mirror
Fatal Error	avale.iat.educacao.ba.gov.br	Linux	mirror
Free MAN (Ly)	www.nkpc.gov.ly/modules/news/i...	Linux	mirror
GHoST61	george.gov.za/gh.html	Linux	mirror
GHoST61	baviaans.gov.za/gh.html	Linux	mirror
gilang	pa-sungguminasa.go.id	Linux	mirror
gilang	matrakab.go.id	Linux	mirror
gilang	kpu-tangerangkab.go.id	Linux	mirror

gilang	www.bekangdam1bbmedan.mil.id	Linux	mirror
Governor	www.izmitmeb.gov.tr/images/uya...	Win 2008	mirror
Group Hp-Hack	www.hu.furg.br	Linux	mirror
Group Hp-Hack	www.darb.furg.br	Linux	mirror
Group Hp-Hack	www.dalcs.furg.br	Linux	mirror
Group Hp-Hack	www.daea.furg.br	Linux	mirror
Group Hp-Hack	www.ctg.furg.br	Linux	mirror
Group Hp-Hack	www.caic.furg.br	Linux	mirror
Group Hp-Hack	www.arca.furg.br	Linux	mirror
Group Hp-Hack	www.cele.furg.br	Linux	mirror
Group Hp-Hack	www.cel.furg.br	Linux	mirror
Group Hp-Hack	www.cdh.furg.br	Linux	mirror
HacKed By LaMiN3 DK	katd.cntq.gob.ve/plugins/dz.txt	Linux	mirror
HacKed By LaMiN3 DK	www.vimeo.cc-vimeuindustriel.fr	Linux	mirror
HacKed By LaMiN3 DK	ccv.cntq.gob.ve/images/dz.txt	Linux	mirror
HacKed By LaMiN3 DK	health.go.ug/index.html	Linux	mirror
HacKed By LaMiN3 DK	secondocomprensivorosolini.gov.it	Linux	mirror
HacKed By LaMiN3 DK	comprensivoprimomazzarino.gov....	Linux	mirror
HacKed By LaMiN3 DK	www.icarenella.gov.it	Linux	mirror
HacKed By LaMiN3 DK	www.stoppacompagnoni.gov.it	Linux	mirror
HacKed By LaMiN3 DK	www.2circolovoghera.gov.it	Linux	mirror
HacKed By LaMiN3 DK	www.iislanciano.gov.it	Linux	mirror
HacKed By LaMiN3 DK	www.itcgtuducabruzzi.gov.it	Linux	mirror
HacKed By LaMiN3 DK	www.icprizzi.gov.it	Linux	mirror
HacKed By LaMiN3 DK	www.icdanti.gov.it	Linux	mirror
HacKed By LaMiN3 DK	www.icsarmaforte.gov.it	Linux	mirror
HacKed By LaMiN3 DK	www.artusiroma.gov.it	Linux	mirror
HacKed By LaMiN3 DK	www.liceobisazza.gov.it	Linux	mirror
HacKed By LaMiN3 DK	www.icgalvaligi.gov.it	Linux	mirror
HacKed By LaMiN3 DK	www.leccediaz.gov.it	Linux	mirror
HacKed By LaMiN3 DK	www.3circolocarmagnola.gov.it	Linux	mirror
HacKed By LaMiN3 DK	www.ddpartannamondello.gov.it	Linux	mirror
HacKed By LaMiN3 DK	www.comprensivomaglie.gov.it	Linux	mirror
HacKed By LaMiN3 DK	www.iisstricase.gov.it	Linux	mirror
HacKed By LaMiN3 DK	istitutocomite.gov.it	Linux	mirror
hatrk	www.jkrmt.gov.my	Linux	mirror
HEXB00T3R	www.ssrkjsw.gov.cn/scan.txt	Win 2003	mirror
HighTech	www.educacaoetecnologia.fe.ufr...	Linux	mirror
HighTech	www.sc.lskjd.gov.cn/index.htm	Win 2003	mirror
HighTech	www.zxft.dllsk.gov.cn/index.htm	Win 2003	mirror
HighTech	lsrd.dllsk.gov.cn/index.htm	Win 2003	mirror
HighTech	xysjpt.lncredit.gov.cn/xylnPub...	Win 2003	mirror
HighTech	www.jiaocheng.gov.cn/jczf/inde...	Win 2003	mirror
HighTech	www.sedputumayo.gov.co/SITIO/s...	Linux	mirror
HighTech	santoantoniodoamparo.mg.gov.br	Linux	mirror
HighTech	juiciosorales.morelos.gob.mx	Linux	mirror
HighTech	labsip.io.usp.br/joomla/config...	Linux	mirror
HighTech	laber.io.usp.br	Linux	mirror

HighTech	www.pyo1.obec.go.th/pyo1/	Linux	mirror
HighTech	www.policiaeconomica.gv.ao	Linux	mirror
HighTech	msh-formation.univ-nantes.fr/j...	Unknown	mirror
HighTech	www.letras.ufrj.br/media/index...	Linux	mirror
HighTech	mjm.shitai.gov.cn/index.htm	Win 2003	mirror
HighTech	www.prefeiturademinacu.go.gov....	Linux	mirror
HighTech	www.unifesp.br/humanas/projeto...	Linux	mirror
HighTech	villanueva.gob.ar/images/hacke...	Linux	mirror
HighTech	www.mfa.go.ke	Linux	mirror
HighTech	www.ct.ufsm.br	Linux	mirror
HighTech	proex.unifesp.br/coexrem/	Linux	mirror
HighTech	www.pyo1.go.th	Win 2008	mirror
HighTech	www.opss.isoc.go.th	Linux	mirror
HighTech	www.alanyadevlethastanesi.gov....	Linux	mirror
HighTech	www.vallefertilsanjuan.gob.ar/...	Linux	mirror
HighTech	www.pranangklao.go.th	Linux	mirror
HighTech	www.litoralalentejano.pcp.pt	Linux	mirror
Hmei7	esteast.unep.ch/x.htm	Win 2003	mirror
Hmei7	www.chem.unep.ch/x.htm	Win 2003	mirror
Hmei7	learning.unog.ch/x.htm	Win 2003	mirror
Hmei7	afics.unog.ch/x.htm	Win 2003	mirror
Hmei7	www.lpeonline.unog.ch/x.htm	Win 2003	mirror
Hmei7	bwc.unog.ch/x.htm	Win 2003	mirror
Hmei7	da.unog.ch/x.htm	Win 2003	mirror
Hmei7	survey.unog.ch/x.htm	Win 2003	mirror
Hmei7	ngo.unog.ch/x.htm	Win 2003	mirror
Hmei7	www.uncc.ch/x.htm	Win 2003	mirror
Hmei7	www.unep.ch/x.htm	Win 2003	mirror
Hmei7	pusterad.mil.id	Linux	mirror
Hmei7	www.turismobinacional.furg.br/...	Linux	mirror
Hmei7	www.tecnologiagestaoambiental....	Linux	mirror
Hmei7	www.sisu.furg.br/x.txt	Linux	mirror
Hmei7	www.sedead.furg.br/x.txt	Linux	mirror
Hmei7	www.sacc-hd.furg.br/x.txt	Linux	mirror
Hmei7	www.ppgalimentos.furg.br/x.txt	Linux	mirror
Hmei7	www.posgeografia.furg.br/x.txt	Linux	mirror
Hmei7	www.petmecanica.furg.br/x.txt	Linux	mirror
Hmei7	www.pedagogia.uab.furg.br/x.txt	Linux	mirror
Hmei7	www.oceanfisquigeo.furg.br/x.txt	Linux	mirror
Hmei7	www.ocbio.furg.br/x.txt	Linux	mirror
Hmei7	www.investigacaonaescola.furg....	Linux	mirror
Hmei7	www.educacaoambiental.furg.br/...	Linux	mirror
Hmei7	www.biologia-aquatica.furg.br/...	Linux	mirror
Hmei7	www.webconfsead.furg.br/x.txt	Linux	mirror
Hmei7	www.upec.furg.br/x.txt	Linux	mirror
Hmei7	www.tscbr.furg.br/x.txt	Linux	mirror
Hmei7	www.numa.furg.br/x.txt	Linux	mirror
Hmei7	www.eqa.furg.br/x.txt	Linux	mirror

Hmei7	www.engenhariaoceanica.furg.br...	Linux	mirror
Hmei7	www.egel.furg.br/x.txt	Linux	mirror
Hmei7	www.eenf.furg.br/x.txt	Linux	mirror
Hmei7	www.educamemoria.furg.br/x.txt	Linux	mirror
Hmei7	www.educacaoinfantilemdebate.f...	Linux	mirror
Hmei7	www.ecodosul.furg.br/x.txt	Linux	mirror
Hmei7	www.direito.furg.br/x.txt	Linux	mirror
Hmei7	www.dialogo.furg.br/x.txt	Linux	mirror
Hmei7	www.coneco.furg.br/x.txt	Linux	mirror
Hmei7	www.cleuzareitora.furg.br/x.txt	Linux	mirror
Hmei7	www.ciscap.furg.br/x.txt	Linux	mirror
Hmei7	www.cip.furg.br/x.txt	Linux	mirror
Hmei7	www.ceperv.furg.br/x.txt	Linux	mirror
Hmei7	www.brinquedoteca.furg.br/x.txt	Linux	mirror
Hmei7	www.blhhu.furg.br/x.txt	Linux	mirror
Hmei7	www.acessoainformacao.furg.br/...	Linux	mirror
Hmei7	www.nutricao.ufpr.br/x.txt	Linux	mirror
Hmei7	www.pgbiocel.ufpr.br/x.txt	Linux	mirror
Hmei7	www.cmr.ensino.eb.br/x.txt	Linux	mirror
Hmei7	avira.si	Linux	mirror
hmezkcq	www.coronelxavierchaves.mg.gov.br	FreeBSD	mirror
hmezkcq	www.camaracxc.mg.gov.br	FreeBSD	mirror
ir4dex	cordillera.gov.ph	Linux	mirror
islamic ghosts team	www.municipiosantiago.gob.ec	Linux	mirror
islamic ghosts team	www.valandovo.gov.mk/x.html	Linux	mirror
islamic ghosts team	www.mcc.gouv.ht/bibliotheque/x...	Unknown	mirror
islamic ghosts team	www.mci.gouv.ht/x.html	Unknown	mirror
Jas0nz666	ges.gov.gh	Linux	mirror
k4L0ng666	tarjeta.cntq.gob.ve/tmp/	Linux	mirror
k4L0ng666	disnakertrans.konaweselatankab...	Linux	mirror
k4L0ng666	bappedasultra.go.id/robots.txt	Linux	mirror
k4L0ng666	www.ministers.sa.gov.au	Linux	mirror
k4L0ng666	premier.sa.gov.au	Linux	mirror
k4L0ng666	www.ppaa.go.tz/robots.txt	Linux	mirror
k4L0ng666	oppy.opp.go.th/admin/news_file...	Linux	mirror
k4L0ng666	www.cohryl.cnh.gob.ve/yenni.txt	Linux	mirror
k4L0ng666	incendios.sirefor.go.cr/robots...	Linux	mirror
k4L0ng666	www2.chainatpao.go.th/robots.txt	Linux	mirror
k4L0ng666	www.electoralmisiones.gov.ar/r...	Linux	mirror
k4L0ng666	servicios.conaliteg.gob.mx/yen...	Linux	mirror
k4L0ng666	portal-joomla.damt.gov.gr/docu...	Linux	mirror
k4L0ng666	www.fonacit.gov.ve/yenni.txt	Unknown	mirror
k4L0ng666	www.fmis.mef.gov.kh/robots.txt	Linux	mirror
k4L0ng666	soyte.hoabinh.gov.vn/syt/robot...	Linux	mirror
k4L0ng666	www.banlueak.go.th/robots.txt	Linux	mirror
k4L0ng666	www.urbanismo.niteroi.rj.gov.b...	Linux	mirror
k4L0ng666	www.funcionjudicial-santodomin...	Linux	mirror
katon	www.itjen.depkes.go.id/itjen/k...	Linux	mirror

KmL!	drssjmvmt.gob.pe	Linux	mirror
KmL!	www.drsveslpp.gob.pe	Linux	mirror
KurdHackTeaM	ihale.ibb.gov.tr/index.html	Win 2003	mirror
KurdHackTeaM	vetistanbul.ibb.gov.tr/index.html	Win 2003	mirror
KurdHackTeaM	wap3.ibb.gov.tr/index.html	Win 2003	mirror
KurdHackTeaM	gencliksporkariyer.ibb.gov.tr/...	Win 2003	mirror
KurdHackTeaM	duyuru.ibb.gov.tr/index.html	Win 2003	mirror
KurdHackTeaM	ismek.ibb.gov.tr/index.html	Win 2003	mirror
KurdHackTeaM	planlama.ibb.gov.tr/index.html	Win 2003	mirror
KurdHackTeaM	ismekbasvuru.ibb.gov.tr/index....	Win 2003	mirror
KurdHackTeaM	smsgateway.ibb.gov.tr/index.html	Win 2003	mirror
KurdHackTeaM	belnet.ibb.gov.tr/index.html	Win 2003	mirror
KurdHackTeaM	ismek2.ibb.gov.tr/index.html	Win 2003	mirror
KurdHackTeaM	ulasim.ibb.gov.tr/index.html	Win 2003	mirror
KurdHackTeaM	bulten.ibb.gov.tr/index.html	Win 2003	mirror
L3oN	www.mkek.gov.tr/Haberler/	Win 2008	mirror
LEONE_PARK	sigmo.ufsc.br	Linux	mirror
LEONE_PARK	neurologia.ufsc.br	Linux	mirror
LEONE_PARK	igti.ufsc.br	Linux	mirror
LEONE_PARK	www.klom.ufsc.br	Linux	mirror
Linuxoid	www.mincom.gov.az	FreeBSD	mirror
lulzperu	www.minjusticia.gob.cl	Linux	mirror
m0y	saltoncsd.ca.gov	Win 2008	mirror
Made In Brazil	www.seduc.pi.gov.br/index.html	Win 2003	mirror
Mafia Hacking Team	nupresswebt.northwestern.edu/i...	Win 2003	mirror
Mafia Hacking Team	www.mardintarim.gov.tr/index.html	Win 2003	mirror
Mafia Hacking Team	www.comune.rivoli.to.it/includ...	Win 2003	mirror
Maxney	www.ad.siemens.com.tw/index.html	Win 2003	mirror
MG-UN17	www.son.gov.ng/index.php/compo...	Win 2008	mirror
moroccan kingdom	www.dgpp-mf.gov.dz	Linux	mirror
moroccan kingdom	www.creg.gov.dz	Linux	mirror
Mr.XHat	mic.gov.sd/home.php	Linux	mirror
Mr.XHat	nceisc.navy.mil.ph/news_conten...	Linux	mirror
Mr-ADeL	viengiamdinhykhoa.gov.vn/dz.html	Linux	mirror
MrWanz	www.mozdata.gov.mz/mozdata/sto...	Win 2003	mirror
MrWanz	www.censusinfo.capmas.gov.eg/n...	Win 2008	mirror
Muzikal_St0rm	www.coesioneterritoriale.gov.it	Linux	mirror
Narkoz ®	www.birecikdh.gov.tr	Linux	mirror
NeT-DeViL	www.coemjr.ufpr.br	Linux	mirror
NeT-DeViL	www.editora.ufpr.br/_capas/	Linux	mirror
NeT-DeViL	www.sig.ufpr.br/index.php3	Linux	mirror
NeT-DeViL	www.nusp.ufpr.br/arqs/	Linux	mirror
NeT-DeViL	www.cmc.ensino.eb.br/apm/	Linux	mirror
NeT-DeViL	www.gea.ufpr.br/arquivos/	Linux	mirror
NeT-DeViL	www.ejeq.ufpr.br	Linux	mirror
NeT-DeViL	www.cem.ufpr.br	Linux	mirror
NeT-DeViL	www.projetofalhas.ufpr.br	Linux	mirror
NeT-DeViL	www.nap.ufpr.br	Linux	mirror

NeT-DeViL	www.hidrologia.ufpr.br/teste.php	Linux	mirror
NeT-DeViL	www.madeira.ufpr.br/web/	Linux	mirror
NeT-DeViL	www.direito.ufpr.br/docs/	Linux	mirror
NeT-DeViL	www.bio.ufpr.br/moodledata/	Linux	mirror
NeT-DeViL	www.cc-talmondais.fr	Unknown	mirror
NeT-DeViL	excops.unep.ch	Linux	mirror
NeT-DeViL	vs.oberwart.gv.at	Linux	mirror
NeT-DeViL	www.maliembassy.us/index.php	Linux	mirror
NeT-DeViL	mairie-alby-sur-cheran.fr	Linux	mirror
NeT-DeViL	www.mairie-salaunes.fr	Linux	mirror
NeT-DeViL	www.arzl-pitztal.tirol.gv.at/s...	Unknown	mirror
NeT-DeViL	www1.inbar.int/flowering/view2...	Win 2000	mirror
NeT-DeViL	www.comune.lasalle.ao.it/en/	Linux	mirror
NeT-DeViL	www.wmatc.gov	Win 2003	mirror
NeT-DeViL	www.cianobacterias.furg.br	Linux	mirror
NeT-DeViL	www.semengo.furg.br	Linux	mirror
NeT-DeViL	www.cppd.furg.br	Linux	mirror
NeT-DeViL	www.peld.furg.br	Linux	mirror
NeT-DeViL	www.senalit.furg.br	Linux	mirror
NeT-DeViL	www.ila.furg.br	Linux	mirror
NeT-DeViL	repository.regione.veneto.it/d...	Linux	mirror
NeT-DeViL	diritto.regione.veneto.it	Linux	mirror
NeT-DeViL	sportellounico.regione.veneto.it	Linux	mirror
NeT-DeViL	web1.regione.veneto.it/cicerone/	Linux	mirror
NeT-DeViL	formazioneinsanita.regione.pug...	Linux	mirror
NeT-DeViL	ecologia.regione.puglia.it	Linux	mirror
NeT-DeViL	pugliacreativa.regione.puglia.it	Linux	mirror
NeT-DeViL	www.cc-pays-des-lacs.fr	Win 2003	mirror
New KilleR	forum.ushaiqer.gov.sa	Linux	mirror
Nob0dy	dalat.gov.vn/web/no.htm	Win 2003	mirror
NoEntry Phc	hdskl.hd.gov.cn/bb.html	Win 2003	mirror
Over-X	www.fnpos.dz/index.html	Win 2003	mirror
Over-X	www.enst.dz/index.html	Win 2003	mirror
Persia Security Group	www.russianembassy.org.il/conf...	Linux	mirror
RainsevenDotMy	e-aduan.mpk.gov.my/_attachment...	Win 2008	mirror
RainsevenDotMy	www.span.gov.my/span_aduan/ind...	Win 2003	mirror
RainsevenDotMy	www.anastacio.ms.gov.br/includ...	Linux	mirror
Red Hat Security Team	www.driveclean.ca.gov/Learn_Mo...	Linux	mirror
rooterror	www.mariajuana.gov.ar	Linux	mirror
rooterror	www.oncativo.gob.ar	Linux	mirror
rooterror	www.oncativo.gov.ar	Linux	mirror
SA3D HaCk3D	tv.shicheng.gov.cn/x.txt	Win 2003	mirror
SA3D HaCk3D	www.zzqx.gov.cn/x.txt	Win 2003	mirror
SA3D HaCk3D	www.glsajj.gov.cn/x.txt	Win 2003	mirror
SA3D HaCk3D	www.ahqccz.gov.cn/x.txt	Win 2003	mirror
SA3D HaCk3D	www.sdai.gov.cn/x.txt	Win 2003	mirror
SaccaFrazi	symbiosis.nre.gov.my/Researche...	Win 2003	mirror
SaccaFrazi	oa.hcedu.gov.cn/index.htm	Win 2003	mirror

SaccaFrazi	rsj.tjhexi.gov.cn/l.txt	Win 2003	mirror
SaccaFrazi	zwgk.tjhexi.gov.cn/l.txt	Win 2003	mirror
SaccaFrazi	ajj.tjhexi.gov.cn/l.txt	Win 2003	mirror
SaccaFrazi	czj.tjhexi.gov.cn/l.txt	Win 2003	mirror
SaccaFrazi	www.hxjw.gov.cn/l.txt	Win 2003	mirror
SaccaFrazi	www.ylhshb.gov.cn/l.txt	Win 2003	mirror
sahrawihacker	camaralambari.mg.gov.br	Linux	mirror
sahrawihacker	www.vallidelmonviso.gov.it	Win 2008	mirror
SanFour25	www.ifamenlinea.go.cr/Dz.php	Unknown	mirror
SanFour25	www.fonctionpublique.gouv.tg/D...	Linux	mirror
Sitozin	mengenhastanesi.gov.tr	Linux	mirror
SKOD	province.rid.go.th/phayao/inde...	Win 2003	mirror
SLYHACKER	hsc.go.ug	Linux	mirror
SLYHACKER	virtualwall.rtarf.mi.th	Linux	mirror
SLYHACKER	thaidarfur980.rtarf.mi.th/pdf/	Linux	mirror
SLYHACKER	th980.rtarf.mi.th/pdf/	Linux	mirror
SLYHACKER	ssc.rtarf.mi.th/Joomla/	Linux	mirror
SLYHACKER	reportsar.rtarf.mi.th	Linux	mirror
SLYHACKER	panumas.rtarf.mi.th/configurat...	Linux	mirror
SLYHACKER	oscsecy.rtarf.mi.th/images	Linux	mirror
SLYHACKER	oig.rtarf.mi.th	Linux	mirror
SLYHACKER	ocompg.rtarf.mi.th/mambo	Linux	mirror
SLYHACKER	occd-thai.rtarf.mi.th/testxoops	Linux	mirror
SLYHACKER	ndc.rtarf.mi.th/NEWS/	Linux	mirror
SLYHACKER	micttc.rtarf.mi.th/eduv9	Linux	mirror
SLYHACKER	medo.rtarf.mi.th/templates	Linux	mirror
SLYHACKER	j5.rtarf.mi.th/cms	Linux	mirror
SLYHACKER	j3.rtarf.mi.th//mootw/	Linux	mirror
SLYHACKER	hqssc.rtarf.mi.th	Linux	mirror
SLYHACKER	ertm.rtarf.mi.th	Linux	mirror
SLYHACKER	eenglish.rtarf.mi.th	Linux	mirror
SLYHACKER	cq80b.rtarf.mi.th	Linux	mirror
SLYHACKER	cecg.rtarf.mi.th/te/	Linux	mirror
SLYHACKER	api.rtarf.mi.th	Linux	mirror
SLYHACKER	afdc-rbs919.rtarf.mi.th	Linux	mirror
SLYHACKER	afdc-ict.rtarf.mi.th	Linux	mirror
SLYHACKER	afdc-gso.rtarf.mi.th/txtfilebb/	Linux	mirror
SLYHACKER	afdc-aecu5.rtarf.mi.th/home	Linux	mirror
SLYHACKER	afdc-1rdo.rtarf.mi.th	Linux	mirror
SLYHACKER	comdiv.rtarf.mi.th	Linux	mirror
SLYHACKER	afdc-mdu25.rtarf.mi.th/news.php	Linux	mirror
SLYHACKER	afdc-mdu12.rtarf.mi.th	Linux	mirror
SLYHACKER	afdc-mdu24.rtarf.mi.th	Linux	mirror
SLYHACKER	www.2gsfma.cbmerj.rj.gov.br/im...	Linux	mirror
SLYHACKER	botinho.cbmerj.rj.gov.br/insbo...	Linux	mirror
SLYHACKER	www.grampiancaredata.gov.uk	Linux	mirror
Soly	www.pdii.lipi.go.id/wp-content...	Linux	mirror
SouTHRaNDA	bdembassyathens.gr	Linux	mirror

StRoNiX	www.instat.gov.al	Win 2003	mirror
syrian hackerzz	www.eda.mohp.gov.eg/index.html	Win 2003	mirror
T0r3x	www.tajjjc.gov.cn/x.txt	Win 2003	mirror
T0r3x	gzpt.lncredit.gov.cn/x.txt	Win 2003	mirror
T0r3x	tp.bjcg.gov.cn/x.txt	Win 2003	mirror
T0r3x	www.jneic.gov.cn/x.txt	Win 2003	mirror
T0r3x	www.yqcq.gov.cn/x.txt	Win 2003	mirror
T0r3x	www.zydj.gov.cn/x.txt	Win 2003	mirror
T0r3x	www.ezbqts.gov.cn/x.txt	Win 2003	mirror
T0r3x	www.langao.gov.cn/x.txt	Win 2003	mirror
T0r3x	job.hnbys.gov.cn/x.txt	Win 2003	mirror
T0r3x	www.bjfpw.gov.cn/x.txt	Win 2003	mirror
T0r3x	www.zzrsc.gov.cn/x.txt	Win 2003	mirror
T0r3x	www.transitofloridablanca.gov.co	Linux	mirror
T0r3x	stolac.gov.ba	Linux	mirror
T0r3x	www.lesko.sr.gov.pl	Linux	mirror
T0r3x	qa.comarb.gov.ar	Linux	mirror
T0r3x	www.hydromet.gov.bz	Linux	mirror
T0r3x	www.nepalpolice.gov.np	Linux	mirror
T0r3x	nph.nepalpolice.gov.np	Linux	mirror
T0r3x	mwrpo.nepalpolice.gov.np	Linux	mirror
T0r3x	mrpo.nepalpolice.gov.np	Linux	mirror
T0r3x	cib.nepalpolice.gov.np	Linux	mirror
T0r3x	www.inc.gov.py	Linux	mirror
T0r3x	www.life.gov.lk	Linux	mirror
T0r3x	www.91circolo.gov.it	Linux	mirror
T0r3x	thutuchanhchinhcaobang.gov.vn	Win 2003	mirror
T0r3x	kptgmawar.kptg.gov.my	Linux	mirror
T0r3x	www.kptg.gov.my	Linux	mirror
T0r3x	juventud.seduca.gov.co	Linux	mirror
T0r3x	intranet.antioquia.gov.co	Linux	mirror
T0r3x	www.juegosuniversitarios.gov.co	Win 2003	mirror
T0r3x	gestionhumana.antioquia.gov.co	Linux	mirror
T0r3x	www.paranacionales.gov.co	Win 2003	mirror
T0r3x	www.camaralencois.sp.gov.br	Linux	mirror
T0r3x	peou.gov.gh	Linux	mirror
T0r3x	www.sanatoriocontratacion.gov.co	Linux	mirror
T0r3x	www.dipaleseng.gov.za	Linux	mirror
T0r3x	educacao.capivari.sp.gov.br	Linux	mirror
T0r3x	core.campobom.rs.gov.br	Linux	mirror
T0r3x	www.sessaaurunca.gov.it	Linux	mirror
T0r3x	www.grazzanise.gov.it	Linux	mirror
T0r3x	www.cellole.gov.it	Linux	mirror
T0r3x	www.unionecso.gov.it	Linux	mirror
T0r3x	www.cancelloedarnone.gov.it	Linux	mirror
TeaM MosTa	www.comune.molinella.bo.it/dz.htm	Win 2008	mirror
TeaM MosTa	dxgt.hnsygt.gov.cn/_data/image...	Win 2003	mirror
TeaM MosTa	cueep194.univ-lille1.fr/dz.htm	Win 2003	mirror

TeaM MosTa	www.ville-laneuveville-devant-...	Win 2003	mirror
TeaM MosTa	esenyurt.meb.gov.tr/ARGE/db/dz...	Win 2008	mirror
TeaM MosTa	www.baglarasm.gov.tr/Editor/as...	Win 2008	mirror
team sality	www.scuolamediaviadeivivai.gov.it	Linux	mirror
team sality	www.primocircolocassino.gov.it	Linux	mirror
Terminal_Pk	www.biwta.gov.bd/index.html	Linux	mirror
The UnderTaker	www.fiat500c.cz/top_daf.asp	Win 2003	mirror
THE-AjaN	tv.kulturturizm.gov.tr/images/	Win 2003	mirror
THE-AjaN	iletisim.kultur.gov.tr/index.html	Win 2003	mirror
THE-AjaN	www.akdeniztarim.gov.tr/aktarim/	Win 2003	mirror
TheWayEnd	malatya-tarim.gov.tr/imgmkl/tw...	Linux	mirror
TheWayEnd	siranhem.gov.tr/index3.php	Linux	mirror
Tn-PiRaTe	redconsejoecuador.gob.ec	Linux	mirror
ToP-TeaM	www.srm.foxconn.com/index.html	Win 2003	mirror
TURK KURSUNU	www.population.gov.za	FreeBSD	mirror
TURK KURSUNU	www.dsd.gov.za	FreeBSD	mirror
TURK KURSUNU	www.chernihiv.mns.gov.ua	Win 2003	mirror
TURK KURSUNU	www.istitutougdulena.gov.it	Linux	mirror
Turkish Energy Team	boletines.cntq.gob.ve/logs/x.htm	Linux	mirror
Turkish Energy Team	informet.cntq.gob.ve/logs/x.htm	Linux	mirror
Turkish Energy Team	altec2012.cntq.gob.ve/logs/x.htm	Linux	mirror
uykusuz001	webebt10.embratel.com.br/Monit...	Win 2000	mirror
Vidson	www.regiontacna.gob.pe/grt/web...	Linux	mirror
Vidson	www.muniprogreso.gob.pe	Linux	mirror
Vidson	www.muniabancay.gob.pe/portal/	Linux	mirror
Vidson	www.municirca.gob.pe	Linux	mirror
VoLcanoHaCkeR	housing-portsaid.gov.eg	Linux	mirror
VoLcanoHaCkeR	zhor.housing-portsaid.gov.eg	Linux	mirror
VoLcanoHaCkeR	sleman.housing-portsaid.gov.eg	Linux	mirror
VoLcanoHaCkeR	savia.housing-portsaid.gov.eg	Linux	mirror
VoLcanoHaCkeR	portps.housing-portsaid.gov.eg	Linux	mirror
VoLcanoHaCkeR	omelmoameneen.housing-portsaid...	Linux	mirror
war0k	tatakota.baubaukota.go.id/x.html	Linux	mirror
war0k	slide.baubaukota.go.id/x.html	Linux	mirror
war0k	setda.baubaukota.go.id/x.html	Linux	mirror
war0k	pkk.baubaukota.go.id/x.html	Linux	mirror
war0k	perijinan.baubaukota.go.id/x.html	Linux	mirror
war0k	bp3m.baubaukota.go.id/x.html	Linux	mirror
way ?????????????	www.ee.furg.br	Linux	mirror
WeWe ArAr	diskes.tanjungpinangkota.go.id	Linux	mirror
WeWe ArAr	dishub.tanjungpinangkota.go.id	Linux	mirror
WeWe ArAr	demo2.tanjungpinangkota.go.id	Linux	mirror
WeWe ArAr	bappeda.tanjungpinangkota.go.id	Linux	mirror
WeWe ArAr	tanjungpinangkota.go.id	Linux	mirror
WeWe ArAr	sample2012.tanjungpinangkota.g...	Linux	mirror
Z3eM 511	www.majmun.gov.sa	Linux	mirror
ZiqoR	bagprojesi.bozkirtarim.gov.tr/...	Linux	mirror
ZiqoR	bozkirtarim.gov.tr/ziqor.txt	Linux	mirror

ZiqoR		edirnedefterdarligi.gov.tr/ziq...	Linux	mirror
ZiqoR		edirneab.gov.tr/ziqor.txt	Linux	mirror
ZoRRoKiN		www.un.org.pl	Linux	mirror
ZoRRoKiN		cscweb.cern.ch/csc2012/gallery...	Linux	mirror
	داعس هكر	www.singburipao.go.th/admini/	Win 2003	mirror

Top Attack 10 Sources	Reports	Attacks	First Seen	Last Seen
069.175.126.170 (US)	1,495,244	135,971	2012-07-11	2012-09-20
037.009.053.002 (RU)	482,733	104,477	2012-09-12	2012-09-19
071.255.142.198 (US)	198,719	101,182	2012-08-22	2012-09-19
061.147.103.098 (CN)	250,935	99,039	2012-09-19	2012-09-19
060.174.198.082 (CN)	264,951	93,439	2012-09-19	2012-09-19
074.055.087.138 (US)	170,317	86,531	2012-09-09	2012-09-20
061.147.068.211 (CN)	323,768	83,678	2012-09-02	2012-09-20
218.095.228.109 (CN)	86,640	73,891	2012-05-02	2012-09-20
069.175.054.106 (US)	745,621	68,856	2012-07-14	2012-09-20
060.214.233.180 (CN)	67,135	67,135	2012-09-19	2012-09-19

Jobs

Hands-on Penetration Testing Support for a two-week On-Site from September 24, 2012 - October 5, 2012. Must be a US Citizen. Please send resume and rate to 911@NetSecurity.com.

Posted by Inno Eroraha [NetSecurity], Founder & Chief Strategist, NetSecurity® Corporation

Junior / Mid-Level Pen Tester

Posted by Terry Bradley, Cyber Security Tester at Big Consulting Firm

If you do not want to receive future emails from us, contact remove@informationwarfarecenter.com