URZ 02/08 – Aktuelles, Tipps und Tricks

In eigener Sache

Liebe Leserinnen und Leser,

wir hoffen, dass Ihnen dieses neue Exemplar von *ATT* zusagt; über jede Anregung und jeden interessanten Tipp von Ihrer Seite freuen wir uns.

Joachim Lammarsch, 1. 3. 2008

INSTMAIL: 3. Schritt der Umstellung von TWIG nach HORDE

Joachim Lammarsch

Wie angekündigt, wurde jetzt TWIG endgültig durch HORDE ersetzt; das Zugangsfenster und der Link zu TWIG wurden entfernt. Der Aufruf von TWIG ist daher jetzt nicht mehr möglich. Auf den jeweiligen Eingangsseiten der virtuellen MAIL-Server (beispielsweise `mail.demo.uni-heidelberg.de`) hatten die Fenster von TWIG und HORDE schon seit Mitte November 2007 ihre Plätze getauscht. Angekündigt war diese Umstellung seit Ende Oktober; nach drei Monaten ist jetzt der Umzug endgültig durchgeführt.
HORDE ist ein mehr als gleichwertiges WWW-Interface, daher sind keine Einschränkungen in der Bedienung zu erwarten. Bestehende Adressbücher können umgezogen werden. Bei Fragen wenden Sie sich bitte an Ihren Mail-Beaufragten, siehe `http://mail.[institutskuerzel].uni-heidelberg.de`.
Mit der Umstellung wurde lediglich ein WWW-Zugang (TWIG) durch einen anderen (HORDE) ersetzt. Nicht betroffen sind daher IMAP- und POP-Zugang, und auch bei der Mail-Box wurde nichts geändert.

TEAM Sicherheit

Patches für schwere Sicherheitslücken in Windows und Office

Kerstin Zapf

Mit den Februar-Patches von Microsoft werden insgesamt 17 Sicherheitslöcher geschlossen, die in Windows und dem Office-Paket von Microsoft auftraten. Das Einspielen der Patches wird dringend empfohlen, da hierdurch auch schwerwiegende Fehler behoben werden, die das Ausführen von schädlichem Programmcode ermöglichen.
Ein Sammel-Patch für den Internet Explorer behebt vier kritische Sicherheitslücken, die das Einschleusen von Schadcode über präparierte Webseiten möglich macht. Ein ähnlicher Fehler im OLE-Protokoll wird durch ein anderes Patch behoben, wobei neben Windows auch Office 2004 für Mac und Visual Basic 6.0 betroffen sind.
Desweiteren wurde ein schweres Sicherheitsloch in den Office-Versionen 2000, XP, 2003 sowie 2004 für Mac entdeckt, während sich in den verschiedenen Word-Versionen ein verwandtes Problem findet: In allen Fällen ist das Ausführen von Schadcode durch manipulierte Dokumente möglich, was nun durch ein Patch verhindert werden kann.
Neben den genannten Fehlerbeseitigungen stellt Microsoft weitere Updates zur Verfügung, die Sicherheitsmängel in Versionen des Publisher, im Windows-WebDAV-Miniredirector, den Internet Information Services und im Active-Directory-Dienst beheben sollen. Eine Übersicht mit ausführlichen Informationen und der Downloadmöglichkeit findet sich hier:

http://www.microsoft.com/germany/technet/sicherheit/bulletins/ms08-feb.mspx

Schwachstelle im Linux Kernel

Joachim Lammarsch

Kürzlich wurde ein neuen lokaler root-Exploit (d. h. Software, welche eine spezifische Schwäche im System ausnutzt) entdeckt, die den Linux-Kernel 2.6.x betrifft. Dabei handelt es sich um eine Überschreitung lokaler Privilegien im Systemaufruf `vmsplice_pipe`, was von *lokalen* Angreifern ausgenutzt werden kann, um root-Zugriff zu erlangen.
Betroffen sind alle Linux-Kernels ab Version 2.6.17 und damit die SuSE/openSUSE-Versionen (10.1, 10.2, 10,3), die das URZ über seine Linux-Software-Verteilung zur Verfügung stellt. Das Problem wird auch von anderen Distributionen (Ubuntu, Fedora, ...) gemeldet.
Für die vom Rechenzentrum angebotenen Distributionen steht unter folgendem Link ein Patch bereit:

ftp://ftp.uni-hd.de/pub/linux/opensuse/update/10.3/

In der neuen Kernel-Version 2.6.24.2 (`http://kernel.org/`) ist der Fehler ebenfalls behoben.

Schwachstellen in Firefox, Thunderbird und SeaMonkey

Joachim Lammarsch

In den Mozilla-Produkten Firefox, Thunderbird und SeaMonkey wurden insgesamt elf Schwachstellen gefunden, die ein entfernter Angreifer dazu ausnutzen kann, beliebigen Skript- oder Programmcode mit den Rechten das Benutzers auszuführen. Schon der Besuch einer manipulierten WWW-Seite kann genügen, den Rechner zu infizieren. Es wird daher empfohlen, die für Firefox aktualisierte Version (2.0.0.12), die unter

http://www.mozilla.com/firefox/

bereitgestellt wird, zu installieren. Distributionen wie openSUSE stellen die neue Version über ihre Update-Mechanismen zur Verfügung.
Die aktualisierten Versionen für SeaMonkey (1.1.8) sowie für Thunderbird (2.0.0.12) stehen ebenfalls jeweils unter folgenden Links zum Download bereit:

http://www.seamonkey-project.org/releases/

http://www.mozilla.com/thunderbird/

Kritische Schwachstellen in Adobe Reader

Joachim Lammarsch

Gleich mehrere kritische Schwachstellen im *Adobe Reader* ermöglichen, feindlichen Programmcode auszuführen. Sie fußen u. a. auf Fehlern bei der Ausführung von Java-Script und können durch manipulierte PDF-Dateien ausgenutzt werden. Hierbei kann schon der Besuch einer vom Angreifer manipulierten WWW-Seite genügen. Ein Exploit ist bereits im Netz erkannt worden.
Gehen Sie daher äußerst vorsichtig mit PDF-Dateien um. Öffnen Sie keine PDF-Dateien, die Sie aus unbekannten oder nicht vertrauenswürdigen Quellen erhalten haben (z. B. per Spam), folgen Sie auch keinem Link auf unbekannte WWW-Seiten.
Installieren Sie am Besten umgehend die vom Hersteller unter untenstehender Adresse bereitgestellte aktualisierte Version (8.1.2) für den Adobe Reader. Eine Aktualisierung der Version 7.0.9 ist ebenso angekündigt.

http://www.adobe.com/go/getreader

TEAM Windows-Systeme

Windows Vista Service Pack 1

Kerstin Zapf

Kürzlich stellte Microsoft das *Service Pack 1* für Windows Vista fertig, das bisher allerdings nur an Gerätehersteller vertrieben wird. Für Privatnutzer sind vorerst nur die Updates erhältlich, die Installationsvoraussetzung hierfür sind. Der Download des Pakets selbst soll aufgrund von Treiberproblemen erst ab Mitte März möglich sein. Hat man die automatische Update-Installation konfiguriert, erfolgt die Belieferung erst Mitte April.
Mit Optimierungen in vielen Bereichen sorgt das SP 1 für verbesserte Geschwindigkeit, Stabilität und Kompatibilität des Betriebssystems. Wesentlich ist u. a. die Erweiterung der Hardware-Unterstützung, die Windows Vista kompatibler macht. Effektiver wird auch der Crack-Schutz, da SP1 zwei wesentliche Tricks zur illegalen Nutzung ohne Lizenz unwirksam macht. Außerdem öffnet sich Vista mit dem SP1 nun auch Drittanbietern. Als Reaktion auf eine Google-Beschwerde ist jetzt zum Beispiel die Einbindung von externen Suchfunktionen möglich, die der Nutzer selbst auswählen kann.
Für einen Überblick über die Neuerungen, die das Service Pack 1 mit sich bringt, bietet sich die Liste der Änderungen im Release Candidate an, da wesentliche Änderungen für die Endversion nicht zu erwarten sind:

http://technet2.microsoft.com/windowsvista/en/library/005f921e-f706-401e-abb5-eec42ea0a03e1033.mspx?mfr=true

TEAM Anwendungssoftware

Linux-Kernel 2.6.24

Jana Motzet

Nach dreieinhalbmonatiger Arbeit wurde nun Version 2.6.24 des Linux-Kernels freigegeben. Vor allem wegen der vorgenommenen Vereinheitlichung der Architekturen i386 und x86_64 zur neuen Architektur x86 stellt dieses Kernel-Update das größte je herausgegebene dar.
Eine zentrale Neuerung bietet die Optimierung des *Completely Fair Scheduler* (CFS). Mit dessen neuer Möglichkeit, nicht nur einzelne Tasks, sondern auch Task-Gruppierungen Prioritäten zuzuordnen, sorgt er dafür, dass der Kernel schneller läuft. Wesentlich ist auch die Optimierung der Speicherverwaltung, die die Fragmentierung des Speichers reduziert. Hierdurch ist auch nach langer Laufzeig noch ausreichend Speicherplatz für Kernelfunktionen vorhanden. Desweiteren wurde die Virtualisierungsfunktion mit Netzwerk- und Prozess-ID-Namensräumen weiter ausgebaut und die Stromsparfunktion *Tickless* ist auf diversen Architekturen (x86-64, PPC, UML, ARM und MIPS) anwendbar.
Unter den zahlreichen neuen Treibern des Kernels 2.6.24 sind auch sieben neue WLAN-Treiber enthalten, sodass eine umfassende Unterstützung aktueller mobiler Hardware gewährleistet ist. Weitere Überarbeitungen umfassen unter anderem die MMC-Schicht, die um die Unterstüzung von SPI und SDIO erweitert wurde. Der USB-Treiber arbeitet nun – in Vorbereitung auf Wireless-USB – mit Autorisierung.
Eine umfassende Liste aller Neuerungen findet sich im Changelog, der über untenstehenden Link zu erreichen ist. Auch der Download des neuen Kernels ist hier möglich:

http://www.kernel.org/

LaTeX: proTeXt 2.1 veröffentlicht

Joachim Lammarsch

Seit Kurzem ist *proTeXt* in der Version 2.1 zum kostenlosen Download verfügbar. Es handelt es sich um eine TeX-Distribution für Windows, die auf *MikTeX* basiert. Mit der neuen proTeXt-Version passte Entwickler Thomas Feuerstack die Distribution der neuen MikTeX-Ausgabe 2.7 an, die vor einigen Wochen erschien.
Die Software ist besonders einfach installierbar: eine Anleitung im PDF-Format ermöglicht dem Benutzer die Installation einzelner Komponenten über Links im Dorkument.
Über folgenden Link ist die proTeXt-Homenapge mit Download-Möglichkeit abrufbar:

http://tug.org/protext

Update-Version KDE 4.0.1 erschienen

Jana Motzet

Mit KDE 4.0.1 ist nun die erste Update-Version für das vor einem Monat erschienene KDE 4.0, verfügbar. Der kosentlose Download ist unter folgendem Link möglich:

http://download.kde.org/download.php?url=stable/4.0.1/

Während neue Funktionen erst mit der für Juni angekündigten Version 4.1 kommen sollen, werden in der jetzigen Update-Version lediglich die bisher festgestellten Fehler behoben. Entscheidend ist hierbei vor allem die Stabilisierung des *Konqueror*. Der Browser soll nun hinsichtlich der HTML-Anzeige besser funktionieren. Ebenso der Flah-Plug-In-Lader und die JavaScript-Engine *KJS* sind von den Korrekturen betroffen. Darüber hinaus wurden laut den Enwicklern einige kleinere Fehler behoben, die die verschiedenen KDE-Komponenten aufwiesen. So wurden unter anderem der Fenstermanager *KWin* sowie die Erkennung von Compositing-Funktionen verbessert. Alle Änderungen sind dem aktuelen Changelog zu entnehmen, der unter untenstehendem Link abrufbar ist:

http://www.kde.org/announcements/changelogs/changelog4_0to4_0_1.php

Neue Langzeitunterstützung: Ubuntu 6.06.2 LTS

Jana Motzet

Mit dem neu erschienenen Ubuntu 6.06.2 LTS hat Canonical nun eine aktualisierte Version der Ubuntu 6.06-Langzeitunterstützung veröffentlicht. Diese enthält alle bis Anfang dieses Jahres vorhandenen Sicherheits-Uptdates, die Ubuntu 6.06 betreffen und umfasst damit über 600 Patches. Im Downloadbereich von Ubuntu kann das Update kostenlos heruntergeladen werden:

http://www.ubuntu.com/getubuntu/download

Durch diese erneuerte Patch-Kompilation müssen nach dessen Installation weniger Updates heruntergeladen werden, sodass Ubuntu 6.06.2 vor allem für Neuinstallationen sinnvoll ist.
Das Update soll der Verbesserung von Stabilität und Kompatibilität von Ubuntu 6.06 LTS dienen. So liegt der Fokus neben den Sicherheits-Updates auf der Optimierung der Hardware-Unterstützung, v. a. bezüglich der unterstützten Server. Zum Beispiel werden Fehler behoben, die mit HPs Pro-Liant-DL3xx-Servern auftauchten. Ausführlichere Informationen zu den vorgenommenen Änderungen können der Ankündigung auf folgendem Link entnommen werden:

http://www.ubuntu.com/news/lts-6.06.2

Termine

Kurse im URZ

Edith Pokrandt

Im aktuellen und dem folgenden Monat beginnen bzw. finden am URZ folgende, chronologisch aufgeführte Kurse statt:

3-Tageskurs: Einführung in die Programmierung mit SAS
Dr. Carina Ortseifen, 12.–14.3.08, V+Ü 9.00–14.00 Uhr
Linux-Treff am URZ
Joachim Lammarsch, 20.03.08, 15.15–17.00 Uhr
Linux-Einführung
Joachim Lammarsch, 27.03.08, 15.15–17.00 Uhr
Linux-Treff am URZ
Joachim Lammarsch, 17.04.08, 15.15–17.00 Uhr

Genauere Informationen und Anmeldung unter:

http://www.urz.uni-heidelberg.de/Ausbildung/Kurse/

Tipps und Tricks

Excel: Hin- und Herspringen zwischen geöffneten Arbeitsmappen

Michaela Wirth

Mit der Tastenkombination `STRG + F6` springen Sie schnell von einer geöffneten Arbeitsmappen zur anderen.

Imperia: Duplikate vom WebServer löschen

Frank Tobian

Problem:

Ich habe ein Dokument umbenannt und es ist jetzt unter verschiedenen Dateinamen auf dem Server.

Lösung:

Holen sie das Dokument mit *Quick Edit* in den Workflow, klicken sie nun auf LIVE LÖSCHEN, um *alle* Varianten des Dokuments vom Server zu löschen. Wenn sie nun das über QuickEdit Importierte freischalten, ist es die einzige Version, die wieder auf dem Server steht.

LaTeX: KILE-Erweiterung für KOMA-Script

Joachim Lammarsch

Frage:

Gibt es für Kile (KDE Latex-Frontend) eine Erweiterung, die die KOMA-Befehle zur Verfügung stellt und vielleicht sogar Format-Wizards hat?

Antwort:

KILE bringt mit Version 1.9.2 Vervollständigungsdateien für die wichtigsten KOMA-Klassen *scrreprt*, *scrbook*, *scrartcl* mit. In der aktuellen openSUSE 10.3-Version ist KILE Version 1.9.3 enthalten. Im Internet ist mittlerweile die Version 2.0 verfügbar, die über folgenden Link kostenlos heruntergeladen werden kann:

http://software.opensuse.org/search?p=1&q=kile&baseproject=openSUSE%3A10.3

Das gab es auch noch

neues Spam-Botnetz entdeckt

Leif Enzmann

Das Unternehmen *Bitdefender*, das sich für Virenschutz einsetzt, warnt vor einem neu entdeckten Spam-Botnetz, das Computer durch Links in Spam-Mails mit Viren infiziert. Die Spammer umgehen dabei URL-basierte Spam-Filter, indem sie keine Links auf die eigenen Webseiten verschicken, sondern solche auf Google-Trefferlisten. Über diese wird der User mit Hinweisen zu expliziten Videos von Prominenten zu den infizierten Webseiten gelockt.

Bei Aufruf der auf den Trefferlisten verlinkten Seiten erfolgt die sofortige Infizierung des PCs mit dem Trojaner Exchanger.A. Dieser lädt anschließend Rootkits und schädliche Programme herunter, über die dann Spam-Mails weiterverschickt werden. Hierdurch breitet sich der Trojaner immer weiter aus. Die Malware wird von Sicherheitsexperten auf dem Provider *Providers Russian Business Network* (RBN) verortet, der bereits vielfach als Plattform für Spam-Mails und Cyberkriminalität in Erscheinung getreten ist.

Weitere Informationen finden Sie in der Warnmeldung von Bitdefender auf untenstehender Seite. Hier findet sich auch ein Link zu einer laufend aktualisierten Liste aktuell verbreiteter Malware.

http://www.bitdefender.de/NW670-de–bitdefender-warnt-vor-spam-botnetz-das-user-mit-videos-von-paris-hilton-und-britney-spears-lockt.html

Microsoft: Visual Studio Express 2008

Jana Motzet

Mit den neuen Express-Versionen zu Microsoft *Visual Studio 2008* sind nun verschiedene Funktionen des Programms zur kostenlosen Nutzung verfügbar.

Neben den Paketen *Visual Basic 2008 Express*, *Visual C# 2008 Express* und *Visual C++ 2008 Express* für Entwickler gibt es das speziell für Web-Enwickler interessante *Visual Web Developer 2008 Express*. Ergänzend sind der SQL Server 1005 Express sowie die *SQL Server Compact Edition* verfügbar.

Gegenüber den älteren Versionen weisen alle Entwicklungsumgebungen einige Neuerungen auf: So bietet die neue Technologie Language Integrated Query (LINQ) für die unterstützten Programmiersprachen C#, C++ und Visual Basic den vereinfachten Datenzugriff, indem SQL-Befehle direkt im Quelltext verwendet werden können. Durch die Unterstützung des Windows Presentation Framework (WPF) ist es Entwicklern außerdem möglich, interaktive Bedienoberflächen zu gestalten.

Der neue Web Developer 2008 Express wartet nun mit einer Split-Screen-Ansicht auf, sodass gleichzeitig der eingegebene HTML-Code und das Ergebnis eingesehen werden können. Außerdem können nun durch ASP.NET AJAX leicht bedienbare Webseiten für alle üblichen Browser erstellt werden. Neu ist auch die Unterstützung von Javascript-Code, die der erweiterte Web-Editor mit sich bringt.

Die 2008-Express-Ausgaben sind laut Windows mit ihren Vorgängerversionen kompatibel und unterstützen die Entwicklung für verschiedene Editionen der Laufzeitumgebung .NET Framework.

Ausführliche Informationen sowie der kostenlose Download sind über folgenden Link erreichbar:

http://www.microsoft.com/germany/express/

Neuartige Phishing-Angriffen auf Kontoinhaber

Jana Motzet

Das Unternehmen für Internet-Sicherheit *Netcraft* berichtet über eine neue Form von Phishing-Attacken, die bereits auf Kunden der *Bank of Lancaster* angewandt wurde. Während das Opfer bei herkömmlichen Phishing-Atacken über einen Link in einer E-Mail zu einer manipulierten Seite gelockt wird, erfolgt hierbei der Betrug per Aufforderung zu einem Anruf.

Es werden E-Mails versandt, die dem Anschein nach von einer Bank stammen. Dem Empfänger wird darin mitgeteilt, seine VISA-Karte sei deaktiviert und möglicherweise illegal genutzt worden. Unter diesem Vorwand wird nun das Opfer dazu aufgefordert, eine vermeintlich kostenfreie Telefonnummer zu wählen um die Bank-Karte wieder zu aktivieren. Wird diese in der Tat gebührenpflichtige Nummer gewählt, so erfolgt die Abfrage persönlicher Daten, die somit für den Missbrauch freigegeben werden.

Selten bleibt dagegen die Phishing-Variante, dass der Betrüger selbst angeblich von der Bank stammende Anrufe zur Datenabfrage durchführt. Wie *Netcraft* anmerkt, biete sich dies allerdings eher zum effektiven Betrug an, da es dem Vorgehen entspreche, dass einige Banken tatsächlich zur Bekämpfung von Betrug durchführen. So setzen diese zum Teil automatische Telefonanrufe zur Überprüfung persönlicher Daten der Karteninhaber ein, sofern verdächtige Transaktionen festgestellt wurden. Hierdurch hat ein Karteninhaber praktisch keine Möglichkeit, sicherzugehen, dass der erhaltene Anruf tatsächlich von seiner Bank stammt.

Ausführliche Informationen finden sich in folgendem Link:

http://news.netcraft.com/archives/2008/02/04/fraudster_using_phone_numbers_to_receive_authentication_details.html

Impressum

Herausgeber:	Rechenzentrum der Universität Heidelberg
Redaktion:	Dr. Carina Ortseifen, Joachim Lammarsch (verantwortlich), Leif Enzmann, Jana Motzet
Verteiler:	`ATT-URZ@urz.uni-heidelberg.de`
Layout:	Luzia Dietsche, Joachim Lammarsch
Produktion:	TEXlive 2007, LATEX 2_ε und pdfTEXk Vers. 3.141592-1.40.3

Namentlich gekennzeichnete Beiträge geben die Meinung der Schreibenden wieder; eine weitere uneingeschränkte Veröffentlichung im WWW ist nicht erlaubt. Die Texte sind nach bestem Wissen erstellt, jedoch kann für die sachliche Richtigkeit keine Garantie übernommen werden. Anregung oder Kritik sowie interessante Beiträge sind jederzeit willkommen. Bitte schicken Sie sie an die Adresse `ATT@urz.uni-heidelberg.de`. Sie können sich bei ATT-URZ durch eine Mail an `listserv@listserv.uni-heidelberg.de` mit dem Inhalt `sub att-urz` einschreiben, oder via:

http://listserv.uni-heidelberg.de/cgi-bin/wa?SUBED1=att-urz&A=1

ATT ist nicht als Alternative zu den BenutzerNachrichten gedacht; vielmehr werden wichtige Artikel in die BN übernommen. Unser Ziel ist lediglich, Ihnen wichtige Informationen möglichst zeitnah zu vermitteln. Zusätzlich fügen wir Tipps und Tricks hinzu, die wir bei unserer Arbeit erfahren haben. Gerne dürfen Sie uns auch Ihre Tipps und Tricks zusenden, die wir dann veröffentlichen.