

UCS 2.2-0 Changelog

Thema:	Protokollierung der Änderungen zwischen den Univention Corporate Server-Versionen 2.1-2 und 2.2-0
Datum:	30. März 2009
Seitenzahl:	25
Versionsnummer:	2975
Autoren:	Univention GmbH feedback@univention.de

Inhaltsverzeichnis

1 Hinweise zum Update	3
2 Univention Managementsystem	3
2.1 Univention Directory Manager	4
2.2 Univention Management Console	6
3 Univention Updater/Softwareverteilung	7
4 Kolab2 für UCS	8
4.1 Kolab2-Groupware-Webclient Horde	9
5 Thin Client-Infrastruktur	11
6 Univention Corporate Desktop	11
7 Services for Windows/Samba	12
8 Univention Active Directory Connector	14
9 Linux Kernel und Kernel-Module	14
10 Xen	15
11 Univention Installer	15
12 Univention Printserver	16
13 Weitere Dienste und Pakete	17
14 Sicherheitsupdates	19

1 Hinweise zum Update

Im folgenden sind die detaillierten Änderungen zwischen den UCS-Versionen 2.1-2 und 2.2-0 beschrieben. Es sollten auch die Hinweise aus dem Dokument **2.2 Release Notes** beachtet werden.

2 Univention Managementsystem

- Mit dem Update auf UCS 2.2 verwenden die Web-Applikationen Univention Directory Manager und Univention Management Console die JavaScript-Bibliothek **dojo Toolkit**. Dadurch ergeben sich einige kleinere Änderungen in der Handhabung. In den nächsten Updates zu UCS wird diese Integration immer weiter ausgebaut (Bug 12849).
- Das JavaScript-Toolkit **dojo** wurde auf Version 1.2.3 aktualisiert (Bug 13034).
- Wird ein DC Backup zum DC Master per `univention-backup2master` hochgestuft, so wird das öffentliche Root-Zertifikat auf dem neuen DC Master jetzt auch per http zur Verfügung gestellt (Bug 11110).
- Die Unterstützung von verschachtelten Gruppen in den LDAP-ACLs kann nun über die Univention Configuration Registry-Variable **ldap/acl/nestedgroups** an bzw. abgeschaltet werden. In großen Umgebungen ist dadurch eine Geschwindigkeitssteigerung in den Verzeichnisdienst-Anfragen zu verzeichnen (Bug 13147).
- Univention Configuration Registry hat ab UCS 2.2 eine weitere Speicherebene (`schedule`). Die Speicherebenen werden folgendermaßen ausgewertet (Bug 12014):
 1. forced (highest)
 2. schedule
 3. ldap
 4. normal (lowest)
- Bei Änderungen der Gruppenmitgliedschaften kann das LDAP-Attribut **memberof** jetzt automatisch über ein neues Overlay-Modul des OpenLDAP-Server aktualisiert werden (Bug 12937).
- Die Module des Univention Directory Listener können jetzt Informationen über den aktuell verwendeten LDAP-Server erhalten, sofern dies für ihre Funktion notwendig ist (Bug 11452).
- Das Replikationsmodul des Univention Directory Listener kann jetzt eine flache Replikation von Benutzern und Gruppen durchführen (Bug 11441).
- Die Berechtigung für die Datei `failed.ldif` wird ab sofort restriktiver vergeben (Bug 13775).
- Teilweise wurde die Datei `failed.ldif` nach dem Wiedereinspielen nicht verschoben. Dieser Fehler wurde behoben (Bug 13777).

2.1 Univention Directory Manager

- Die Sprache des Univention Directory Manager ist jetzt bei der Anmeldung wählbar (Bug 13011).
- Die englischsprachige Übersetzung des Univention Directory Manager wurde überarbeitet (Bug 13369).
- Der Pflichtfelder eines Univention Directory Manager-Modul können über Univention Configuration Registry-Variablen konfiguriert werden. Bspw. kann der Vorname im Benutzermodul über die UCR-Variable `directory/manager/web/modules/users/user/properties/firstname/required` als Pflichtfeld definiert werden (Bug 12876).
- Die Felder für eine Suche nach Nutzern oder Gruppen können über UCR-Variablen der Form `directory/manager/web/modules/MODUL/properties/FELD/dontsearch` eingeschränkt werden (Bug 12876).
- Die Standardsucheigenschaften der einzelnen Univention Directory Manager-Module können nun mittels Univention Configuration Registry-Variablen in der Form `directory/manager/web/modules/MODUL/search/default=EIGENSCHAFT` festgelegt werden (Bug 3363).
- Eine Abmeldung am Univention Directory Manager führt nun direkt zur Anmelde-
maske, ohne dass der Benutzer einen separaten Link aufrufen muss (Bug 11141).
- Ein Session-Timeout im Univention Directory Manager führt nun direkt zur Anmelde-
maske, ohne dass der Benutzer einen separaten Link aufrufen muss (Bug 11344).
- Bei der Auswahl einer anderen Domain oder eines anderen Pfades im Suchdialog bleiben die Eingaben des Benutzers erhalten (Bug 10277).
- Im Univention Directory Manager-Webfrontend wurde die automatische Ausführung der Suchfunktion aktiviert. Diese kann generell (`directory/manager/web/modules/autosearch`) oder pro Modul (`directory/manager/web/modules/MODUL/search/autosearch`) mittels Univention Configuration Registry konfiguriert werden (Bug 11463).
- Der Standard-Timeout für Univention Directory Manager-Sitzungen wurde von 5 auf 15 Minuten erhöht. Ist der aktuelle Wert noch auf 5 Minuten gesetzt, wird dieser automatisch bei der Installation des Univention Directory Manager-Pakets auf 15 Minuten verändert (Bug 11343).
- Die Einstellung **Samba-Schreibzugriff** wurde standardmäßig aktiviert und vom Samba-Allgemein- zum Samba-Rechte-Tab verschoben (Bug 3782).
- Verweise auf Univention Admin wurden im Einstellen-Modul des Univention Directory Manager durch Univention Directory Manager ersetzt (Bug 10042).
- Die Meldung bei einem fehlerhaften Login war nicht konsistent zwischen der deutschen und englischen Übersetzung. Dieser Fehler wurde behoben (Bug 13101).
- Verweise auf Univention Admin im Univention Directory Manager wurden durch Univention Directory Manager ersetzt (Bug 13114 und Bug 10301).

- Der Seitentitel, der bei einem Fehler/Traceback angezeigt wird, wurde auf Univention Directory Manager geändert (Bug 10097).
- Die Startseite nach einer erfolgreichen Anmeldung am Univention Directory Manager wurde um Grafiken erweitert (Bug 8443).
- In der Ergebnisliste einer Suche wird die Spalte mit der gesuchten Eigenschaft nicht mehr angezeigt, wenn diese mit der identifizierenden Eigenschaft übereinstimmt. Zum Beispiel wird die Spalte Benutzername nicht mehr für Benutzer erneut angezeigt (Bug 13131).
- Navigation und Assistenten der Webadministration verwenden jetzt JavaScript zur dynamischen, mehrseitigen Anzeige von Suchergebnissen (Bug 13032).
- Die voreingestellte Anzahl von Suchergebnissen in Navigation und Assistenten wurde auf 10 reduziert. Die Anzahl kann über Univention Configuration Registry-Variablen (`directory/manager/web/modbrowse/defaults/visible-results`, `directory/manager/web/modwizard/defaults/visible-results`) verändert werden (Bug 13032).
- Bei der Verwendung Univention Directory Manager-CLI konnte es beim Hinzufügen von Richtlinien-Verknüpfungen zu einem Traceback kommen, wenn die betreffende Richtlinie bereits mit dem Ziel-Objekt verknüpft war. Dieser Fehler wird jetzt abgefangen (Bug 11699).
- Im Univention Directory Manager werden jetzt erweiterte Einstellungen in der Standardeinstellung nicht mehr angezeigt. Beim Bearbeiten eines Objektes mit Univention Directory Manager wird eine Checkbox angezeigt mit der die erweiterten Einstellungen angezeigt werden. Per Univention Configuration Registry kann diese Checkbox global über `directory/manager/web/modules/advancedview` oder Modul-basiert über `directory/manager/web/modules/MODUL/advancedview` bspw. `directory/manager/web/modules/users/user/advancedview` aktiviert oder deaktiviert werden. Auch kann per Univention Configuration Registry definiert werden, welche Reiter in der normalen Ansicht oder nur in der erweiterten Ansicht zu sehen sind, bspw. `directory/manager/web/modules/users/user/layout/Windows/advanced=True` (Bug 13182).
- Die Reihenfolge der Menüeinträge im Univention Directory Manager wurde angepasst, so dass nun die LDAP-Navigation und die eigenen Benutzereinstellungen unterhalb der Assistenten zu finden sind (Bug 13180).
- Der Menüeintrag für die Bearbeitung des eigenen Benutzerkontos wurde in **Mein Konto** umbenannt (Bug 13176).
- Die Widgets in der Assistenten-Suche im Univention Directory Manager wurden neu ausgerichtet (Bug 13160).
- Unter bestimmten Umständen war die Breite der Reiter im Univention Directory Manager größer als die vorgegebene Breite, dadurch konnte es zu Darstellungsfehlern im Internet Explorer kommen. Dieser Fehler wurde behoben (Bug 13121).

- Die Benutzereinstellungen **Heimatverzeichnisfreigabe** und **Pfad der Heimatverzeichnisfreigabe** wurden in **Heimatverzeichnisfreigabe** und **Freigabe, auf der das Heimatverzeichnis des Benutzers liegt** umbenannt (Bug 12813).
- Das generische Rechner-Modul (computers/computer) enthält jetzt auch das Beschreibungsfeld (description) (Bug 7509).
- Im memberUid-Attribut einer Gruppe werden nur noch Benutzer und Rechner mit ihrer echten **uid** gespeichert (Bug 12644).
- Wurde bei einem Rechner-Objekt die IP-Adresse geändert, so wurde nicht immer die IP-Adresse des DHCP-Objekts mitgeändert. Dieser Fehler wurde behoben (Bug 9908).
- IMAP-Folder im Univention Directory Manager können ab sofort auch im Multiedit-Modus editiert werden (Bug 11674).
- Kam es beim Anlegen eines Benutzers im Univention Directory Manager zu einer Kollision mit einem bereits existierenden Benutzernamen, wurde der neue Benutzer nach dem Anpassen des Benutzernamens mit falschem Heimatverzeichnis angelegt. Dieser Fehler wurde jetzt behoben (Bug 11813).
- In den Bugreport E-Mails des Univention Directory Manager wird jetzt auch die Versionsnummer aufgeführt. Zusätzlich kann der Empfänger dieser E-Mails per Univention Configuration Registry konfiguriert werden (Bug 13072):

```
univention-config-registry set \  
  directory/manager/web/feedback/description="Univention Feedback" \  
  directory/manager/web/feedback/mail="feedback@univention.de"
```

- Das Tool univention-sync-memberuid sortiert jetzt die Listen der Gruppenmitglieder bevor diese verglichen werden (Bug 12901).
- Der Reiter für die erweiterten Samba-Rechte wurde überarbeitet (Bug 5508).
- Diverse Meldungen im Univention Directory Manager wurden neu ausgerichtet (Bug 13284).
- Es wird jetzt eine ausführliche Meldung inkl. Hinweis-Ikon angezeigt, wenn eine Suche im Univention Directory Manager erfolglos war (Bug 13289).
- Das Setzen eines Windows Terminal Server Profilpfads mit Hilfe von Univention Directory Manager hatte unter bestimmten Umständen keine Auswirkung. Dieser Fehler wurde behoben (Bug 13203).
- Wird Univention Directory Manager in einer auf dem System nicht vorhandenen Sprache gestartet, so wird Englisch als Standardsprache verwendet (Bug 13428).

2.2 Univention Management Console

- Die Sprache von Univention Management Console ist jetzt bei der Anmeldung wählbar (Bug 13011).

- Der Timeout für Univention Management Console-Sitzungen wurde von 5 auf 15 Minuten erhöht. Ist der Timeout noch auf 5 Minuten gesetzt, wird dieser automatisch bei der Installation des Univention Management Console-Pakets auf 15 Minuten verändert (Bug 11343).
- Einige Verbesserungen wurden in den internen Strukturen von Univention Management Console durchgeführt (Bug 12534, 13152).
- Ein Traceback, der nach der erfolgreichen Installation eines Softwarepakets aufgetreten ist, wurde behoben (Bug 12924).
- Es wurden Stylesheet-Anpassungen für Hyperlinks vorgenommen (Bug 13234).
- In den Bugreport E-Mails von Univention Management Console wird jetzt auch die Versionsnummer aufgeführt. Zusätzlich kann der Empfänger dieser E-Mails per Univention Configuration Registry konfiguriert werden (Bug 13072):

```
univention-config-registry set \  
  umc/web/feedback/description="Univention Feedback" \  
  umc/web/feedback/mail="feedback@univention.de"
```

- Die englische Übersetzung der Univention Management Console wurde überarbeitet (Bug 13407).
- Univention Management Console wurde um grundlegende Mechanismen erweitert, die für die Auslieferung beliebiger Daten zum Browser wie z.B. dynamisch generierter Bilder oder Daten für das Ajax-Framework benötigt werden (Bug 13259).
- Wird Univention Management Console in einer auf dem System nicht vorhandenen Sprache gestartet, so wird Englisch als Standardsprache verwendet (Bug 13428).
- Univention Management Console verwendet jetzt das Rechnerzertifikat aus dem Verzeichnis `/etc/univention/ssl/<hostname>.<domainname>` (Bug 13598).

3 Univention Updater/Softwareverteilung

- Die Informationen für die Paketquellen zum Installieren und Aktualisieren von Software (`/etc/apt/sources.list`) werden ab sofort über den Univention Configuration Registry-Mechanismus verwaltet. Dabei wird die vorhandene Datei `sources.list` beibehalten. Die Paketquellen werden ab sofort automatisiert in den Dateien unterhalb von `/etc/apt/sources.list.d` geschrieben. Eigene Paketquellen können in eigenen Dateien unterhalb dieses Verzeichnisses abgelegt werden oder auch weiterhin in der Datei `/etc/apt/sources.list` (Bug 11991).
- Die Verzeichnisstrukturen der Repository-Server wurde denen von `apt.univention.de` angepasst. Damit ist es jetzt möglich ein lokales Repository durch Synchronisation von `http://apt.univention.de` zu erzeugen. Über Univention Configuration Registry-Variablen kann definiert werden welche Repositories synchronisiert werden sollen (Bug 12511).

- Um auch ältere UCS-Versionen in ein lokales Repository synchronisieren zu können, kann die älteste und die neueste Version per Univention Configuration Registry-Variable gesetzt werden (`repository/mirror/version/start` und `repository/mirror/version/end`) (Bug 13177).
- Der Update-Server wird nicht mehr in der Univention Configuration Registry-Variable `update/server` eingetragen. Stattdessen wird die Univention Configuration Registry-Variable `repository/online/server` verwendet. Ist das System selbst ein Repository-Server wird die Quelle für die Repository-Synchronisation in der Univention Configuration Registry-Variable `repository/mirror/server` definiert (Bug 13220).
- Das Programm `univention-actualise -check` bricht nun nicht mehr ab, wenn es in einer nicht englischen Umgebung gestartet wird (Bug 10158).
- Ab UCS 2.2 können die Release-Updates direkt aus dem Online Repository installiert werden (Bug 12297):

```
univention-updater net
```
- Zur Migration der alten Repositories wird das Programm `univention-repository-migrate` mitgebracht (Bug 13472).

4 Kolab2 für UCS

- Mit der Univention Configuration Registry-Variable `mail/maps/canonical/recipient/classes` kann nun konfiguriert werden, ob das Canonical-Mapping des Postfix-Dienstes auf die Empfänger-Informationen im Envelope und/oder Mail-Header angewendet werden. Mögliche Einstellungen sind **`envelope_recipient`** und **`header_recipient`** (Bug 13217).
- Mit Hilfe des Paket **`univention-ldap-addressbook-sync`** können die Benutzer, Gruppen und Mailinglisten aus dem Verzeichnisdienst in ein globales Kolab-Adressbuch auf den IMAP-Server synchronisiert werden (Bug 12377).
- Die automatische Terminannahme funktioniert standardmäßig nur für die installierte Mail-Domäne. Mit den folgenden Schritten kann ab UCS 2.2 auch die automatische Terminannahme für weitere Mail-Domänen aktiviert werden (Bug 6201):

```
adduser --quiet --system \  
    --home /var/lib/univention-kolab2cal- $\$$ NEW_DOMAIN kolab2cal  
  
PASSWD_CRYPT=$(mkpasswd --hash=md5 -s < /etc/kolab2cal.secret)  
  
usermod -p "$PASSWD_CRYPT" kolab2cal  
  
usermod -l kolab2cal@ $\$$ NEW_DOMAIN kolab2cal  
  
eval $(univention-config-registry shell)  
  
univention-config-registry set \  
    mail/cyrus/imap/admins="$mail_cyrus_imap_admins kolab2cal@ $\$$ NEW_DOMAIN"
```

4.1 Kolab2-Groupware-Webclient Horde

- Die einzelnen Horde-Applikationen wurden intern auf das Horde-Webmailer Paket umgestellt. Die Einzelanwendungen, wie truba oder kronolith werden nur noch im Gesamtpaket Horde-Webmailer supportet (Bug 11969).
- Horde wurde auf die aktuelle Version Horde Webmailer 1.1.1 aktualisiert. Dadurch sind die Standard-Applikationen MIMP und DIMP ebenfalls verfügbar (Bug 11403).
- Wenn ein Benutzer Zugriff auf mehrere IMAP Adressbücher besitzt, so wurden fälschlicherweise nur die Adressen aus einem Adressbuch angezeigt (Bug 11661).
- Über die UCR-Variable `horde/webroot` kann der Pfad von Horde im Apache dynamisch angepasst werden (Bug 11853).
- Die `.svn`-Verzeichnisse wurden aus dem Paket ***univention-kolab2-webclient*** entfernt (Bug 11974).
- Die Patches aus den existierenden Horde-Modulen wurden in das Paket ***horde-webmailer übernommen*** (Bug 11975).
- Das temporäre Verzeichnis, in dem Horde Daten speichert, wurde fest auf `/var/cache/horde` gesetzt (Bug 11984 und Bug 12186).
- Das Skript `/usr/share/univention-kolab2-webclient/syncml_reset_user.sh` wurde an die neue Horde-Version angepasst (Bug 12187).
- Eine fehlende Paketabhängigkeit konnte zu Fehlern während der Installation des Pakets ***univention-kolab2-webclient*** führen. Die Abhängigkeit auf das Paket ***whois*** wurde zu ***univention-kolab2-webclient*** hinzugefügt (Bug 12277).
- Die Größen der Tabellenspalten in den SyncML-Tabellen der Horde-Datenbank wurden nur während der Neuinstallation angepasst, nicht aber bei einer Paketaktualisierung. Dadurch konnten bestimmte SyncML-Mapping-Einträge nicht geschrieben werden. Die Größen werden jetzt während der Aktualisierung angepasst (Bug 12346).
- Das Logging für SyncML wurde erheblich erweitert. Über die UCR-Variable `horde/sync/debug` kann es aktiviert werden. Für jeden Synchronisationsvorgang wird dann im Verzeichnis `/var/log/horde/sync` ein Unterverzeichnis angelegt, das die erzeugten Logdateien enthält. Das Log-Verzeichnis kann über die UCR-Variable `horde/sync/debugdir` angepasst werden (Bug 12368).
- Ein Fehler in der JavaScript-Datei `time_picker.js` führte dazu, dass der Internet Explorer das Zeitauswahlfeld nicht korrekt dargestellt hat. Dieser Fehler wurde behoben (Bug 12347).
- Der Standard-Kalender und das Standard-Adressbuch werden nun beim Anlegen eines Nutzer gesetzt (Bug 12084).
- Die SyncML-Implementierung überprüfte die Inhalte auf dem IMAP-Server nur während eines Synchronisationsvorgangs, so dass eine zweimalige Synchronisation nötig war, um alle Änderungen zu übertragen. Dieser Vorgang wurde so geändert, dass bereits nach dem ersten Synchronisationsvorgang die Synchronisation vollständig ist (Bug 12127).

- Änderungen an den uidvalidity-Werten auf dem IMAP-Server führten zum erneuten Hinzufügen und damit einer zu einer Verdopplung aller Inhalte des betroffenen IMAP-Ordners auf Geräten, die die SyncML-Schnittstelle verwenden. Dieser Fehler wurde behoben (Bug 12367).
- Die Horde-Komponente **Kronolith** zählte wöchentliche Serientermine falsch, die nach einer bestimmten Anzahl an Wiederholungen gestoppt werden sollten. Dieser Fehler wurde behoben (Bug 12683).
- Die Horde-Komponente **Turba** zeigte in der Adressbuchübersicht nichts an, wenn ein Kontakt keinen Vor- oder Nachnamen besitzt. Zusätzlich wird jetzt das Kontakt-Feld Organisation ausgelesen und angezeigt (Bug 12618).
- Die Horde-Komponente **Kronolith** ermöglicht es jetzt Terminerinnerungen 0 Minuten vor dem Termin anzulegen (Bug 12553).
- Die Horde-Komponente **Kronolith** zeigt Termine, die von anderen Clients, wie Kontakt, als frei gekennzeichnet sind, nicht mehr durchgestrichen an. Die Textdekoration wurde wiederhergestellt und stattdessen der Parser für das Kolab-Datenformat korrigiert (Bug 12619).
- Die Horde-SyncML-Implementierung kann momentan große Nachrichten nicht auf mehrere Pakete aufteilen, um Clients bedienen zu können, die nur kleine Pakete empfangen können. Es wurde eine Lösung geschaffen, die Beschreibungen/Notizen für den mobilen Client kürzt, um den betroffenen Kontakt/Termin in einem Paket übertragen zu können (Bug 12706).
- Die Horde-Komponente **ingo-vacation** ermöglicht die Verwaltung von Abwesenheitsbenachrichtigungen in einer separaten Oberfläche. Über die Univention Configuration Registry-Variable [horde/ingo-vacation/alias](#) kann definiert werden über welchen Pfad die Oberfläche zur Verfügung gestellt wird (Standard: [/vacation](#)) (Bug 12329).
- Weitere Univention Configuration Registry-Variablen wurden mit Beschreibungen versehen, die in der Univention Management Console angezeigt werden (Bug 12496).
- Die MIME-Bibliothek erzeugte Text-Ausgaben, die vom Webbrowser interpretiert wurden. Dieses Sicherheitsproblem wurde beseitigt (CVE-2008-3823).
- Ein Cross-Site-Scripting-Problem mit HTML-Mails wurde behoben (CVE-2008-3824).
- Der Kolab2-Webmailer hat nun neue Abhängigkeiten auf
 - expect (Bug 12300)
 - php5-ldap (Bug 10089)
 - gnupg (Bug 9182)
- Die Logdatei [/var/log/horde/horde3.log](#) wird ab sofort per logrotate rotiert (Bug 12600).
- Das Listener-Modul für das Anlegen der Kolab2-Webclient-Eigenschaften der Benutzer wird nun auch beim Modifizieren der Benutzerobjekte im Univention Directory Manager aufgerufen, sofern die primäre E-Mail-Adresse geändert wurde (Bug 10752).

- Einige fehlende Grafiken für das Kolab2-Webclient-Thema **univention** wurden hinzugefügt (Bug 10346).

5 Thin Client-Infrastruktur

- Der Kernel für die Thin Client-Systeme wurde auf Version 2.6.28.2 aktualisiert. Bei der Installation wird der vorherige 2.6.18er Kernel deinstalliert. Falls der alte Thin Client-Kernel weiterverwendet werden soll, so kann das Paket **univention-client-kernel-image** auf hold gesetzt werden (Bug 13245):

```
echo "univention-client-kernel-image hold" | dpkg --set-selections
```

- Das Paket **univention-thin-client-flash** wird jetzt auf der Installations-DVD mit ausgeliefert (Bug 13095).
- Während des Boot-Vorgangs der Thin Client-Umgebung auftretende udev-Fehlermeldungen wurden entfernt (Bug 11634).
- Die Pakete **univention-thin-client-basesystem** und **univention-thin-client-tools** haben jetzt eine Abhängigkeit auf das Paket **python-univention-debug** (Bug 13593).
- Die debconf-Datei **config.dat** innerhalb der Thin Client-Umgebung wird jetzt als Konfigurationsdatei gepflegt und während des Updates nicht überschrieben (Bug 13578).

6 Univention Corporate Desktop

- Der Webbrowser **Firefox** hat nun eine Abhängigkeit auf ein TrueType-Font-Paket, entweder **ttf-dejavu** oder **ttf-dustin** (Bug 13281).
- Das Flash-Plugin 9 kann nun wieder mit **univention-flashplugin** installiert werden (Bug 12919).
- Kontakt wurde auf die Version 3.5.10.enterprise.0.20090206.922263-kk2 aktualisiert. Unter anderen sind folgende Verbesserungen enthalten (Bug 12922):
 - Verbesserungen in der Kompatibilität zu Outlook. Diese betreffen primär den Umgang mit Anhängen und Einladungen zu Terminen.
 - Die graphische Oberfläche zur Bearbeitung von Verteilerlisten wurde verbessert.
 - Erweiterungen und Verbesserungen im Umgang mit verschlüsselten Mails (PGP und S/MIME) wurden integriert.
 - Verbesserung der Stabilität.
- Der Webbrowser **Firefox** startet nun mit der eingestellten Sprache des Benutzers, falls diese Sprache nicht bekannt ist, so wird Firefox in Englisch gestartet. Standardmäßig werden Sprachpakete für die Sprachen Deutsch, Englisch und Französisch installiert. Weitere Sprachpakete können von der Webseite

<http://releases.mozilla.org/pub/mozilla.org/firefox/releases/3.0.6/linux-i686/xpi/> bezogen werden (Bug 11603).

- Während der Installation oder der nachträglichen Anpassung der Tastatureinstellungen über **univention-system-setup** wird das Tastaturlayout auch für den X-Server übernommen (Bug 11680).
- FreeNX wurde auf Version 0.7.1 aktualisiert (Bug 8746).
- Firefox steht nun in Version 3.0.6 zur Verfügung (Bug 12920).

- OpenOffice.org wurde auf Version 3.0.1 aktualisiert. Aufgrund eines Fehlers in der OpenOffice.org Version 2.4 kann es zu Problemen bei der Betrachtung von Dokumenten kommen, die mit OpenOffice.org 3.0 erstellt wurden. Demnach sollten nach Möglichkeit alle Systeme in kurzer Zeit aktualisiert werden. Falls bei dem Release Update von UCS OpenOffice.org nicht aktualisiert werden soll, so kann das Paket mit dem folgenden Befehl auf hold gesetzt werden (Bug 12917):

```
echo "openoffice.org-base hold" | dpkg --set-selections
```

- Die SUN Java Pakete wurden auf Version 6.07-3 aktualisiert. Sollte eine Aktualisierung nicht erwünscht sein, so kann mit dem folgenden Befehl das automatische Update verhindert werden (Bug 11140):

```
echo "univention-java hold" | dpkg --set-selections
```

Kommende Sicherheits-Updates für UCS 2.2 werden nur noch für Java 6 bereitgestellt werden, die alten Java-Pakete sollten deshalb nach Möglichkeit deinstalliert werden.

- Die Desktopumgebung KDE wurde auf die Version 3.5.10 aktualisiert (Bug 12918).
- Das X-Window-System **X.org** wurde auf die Version 7.3 aktualisiert (Bug 12921).
- Sofern die Startseite des Webbrowsers Firefox nicht verändert wurde, wird diese während der Aktualisierung auf http://www.univention.de/ucd-welcome-2_2-0.html gesetzt (Bug 13644).
- Ein Fehler in der GDM-Autostart-Konfiguration wurde behoben (Bug 13082).

7 Services for Windows/Samba

- Samba wurde auf Version 3.2.8 aktualisiert (Bug 11406). Im folgenden ein Auszug aus den Änderungen gegenüber Samba 3.0.30 aus UCS 2.1-2:
 - Die Limits von 1024 Zeichen (bzw. Bytes) für Pfade und von 256 Zeichen (bzw. Bytes) für Verzeichnis und Dateinamen wurden aufgehoben. Statt dessen wird nun die Einstellung `MAX_PATH` des Betriebssystems verwendet.
 - Samba bietet jetzt Support für den Einsatz als Samba-Fileserver Cluster. Durch die Verwendung der Samba Clustered TDB (CTDB) in Kombination mit einem Clustered Filesystem (beispielsweise GFS2 oder OCFS2) werden Samba-Fileserver so zu einer Option in Umgebungen, die den Einsatz hochverfügbarer Fileserver erfordern. Der Support ist vorerst noch als experimentell eingestuft.

- Samba unterstützt jetzt die Speicherung von NTFS Alternate Data Streams in Extended Attributes auf Samba-Fileservern.
 - Die CIFS-Unix-Erweiterungen wurden verbessert.
 - Samba unterstützt jetzt die Kerberos-Authentifizierung von Windows Vista Clients.
 - Ein Problem in der Kerberos-Authentifikation bei Zugriff auf CIFS-Dateisysteme wurde behoben.
 - Samba bietet jetzt Unterstützung für den verschlüsselten Transport von SMB-Daten zwischen Client- und Server-Komponenten.
 - Samba liefert ein neues VFS Modul zur Analyse von SMB Datenverbindungen mit.
 - Winbind unterstützt jetzt die Auflösung von Gruppen in Gruppen Mitgliedschaften über den Unix Nameservice Switch (NSS).
 - Samba unterstützt jetzt Vertrauensstellungen zwischen Samba und Windows 2008 ADS-Domänen.
 - Samba bietet jetzt auch die Möglichkeit, Client-Systeme durch Kommandos ferngesteuert in Samba-Domänen zu joinen bzw. aus einer Domäne herauszunehmen.
 - Im Zuge der konzeptionellen Erweiterungen für Samba 4 wurde in Samba eine interne Registry eingeführt, die perspektivisch Änderungen an allen Samba Konfigurationsparametern über Funktionsaufrufe von der Kommandozeile erlauben wird. Univention Corporate Server macht vorerst noch keinen Gebrauch von dieser Technik.
 - Samba unterstützt jetzt server- und clientseitig IPv6.
- Die Lizenz der Pakete **univention-samba** und **univention-winprinters** wurde von GPL-2 auf GPL-3 geändert, da der enthaltene Programmcode die Samba Bibliotheken verwendet und Samba jetzt die GPL in der Version 3 verwendet (Bug 12895).
 - Die Samba-Option **domain logons** kann jetzt über die UCR-Variable `samba/domain/logons` gesetzt werden (Bug 12406).
 - In der PAM-Konfiguration von Samba wird nun der PAM-Stack **common-password** eingebunden und nicht mehr **common-passwd** (Bug 12830).
 - Die Synchronisation der Samba-Netlogon-Skripte kann ab sofort per UCR-Variable `samba/netlogon/sync` gesteuert werden (Bug 12178). Die folgenden Werte werden dabei unterstützt:
 - **sync**
Die Netlogon-Skripte werden per `rsync` mit dem Parameter `-delete` vom Master auf das lokale System synchronisiert. Auf dem Master nicht mehr vorhandene Dateien werden lokal gelöscht.
 - **emphdownload**
Das Synchronisationstool `rsync` wird ohne den Parameter `-delete` aufgerufen, wodurch Dateien nur heruntergeladen und ggf. überschrieben werden. Es werden jedoch keine Dateien gelöscht.

- **none**

Die Synchronisation ist deaktiviert.

- Lokale Einstellungen für Samba und Samba-Shares können jetzt über Univention Configuration Registry-Variablen vorgenommen werden (Bugs 12089, 12045, 12024).
- Das Paket **samba4wins** wurde für UCS gebaut. Nach der Installation des Meta-Paket **univention-samba4wins** kann die Konfiguration über das UCS-Managementsystem vorgenommen werden (Bug 5185).

8 Univention Active Directory Connector

- Für eine einfachere Konfiguration des Univention Active Directory Connectors steht jetzt ein Univention Management Console-Modul zur Verfügung, welches beim Setzen der grundlegenden Einstellungen unterstützt (Bug 8736).
- Die Hilfeausgabe des Befehls `univention-adsearch` verwies noch auf `univention-baseconfig` (Bug 11285).
- Die Container **cn=nagios** und **cn=samba** in UCS und **ou=Grp Policy Users** in Active Directory wurden in die Liste der ignorierten Container aufgenommen, Änderungen in/an diesen Objekten werden bei Verwendung des Default-Mappings nicht mehr synchronisiert (Bug 11700).
- Bei der Synchronisation von Gruppenmitgliedschaften wurde eine potentiell fehlerhafte Behandlung ignorierte Gruppenmitglieder beseitigt (Bug 13056).

9 Linux Kernel und Kernel-Module

- Der 2.6.26er Kernel wurde in UCS 2.2 integriert. Während der Aktualisierung auf UCS erfolgt automatisch eine Aktualisierung des 2.6.24er Kernel auf den 2.6.26er Kernel. Falls dies nicht erwünscht ist, so können die Kernel Meta Pakete auf **hold** gesetzt werden (Bug 12908), bspw.:

```
echo "univention-kernel-image-2.6.24 hold" | dpkg --set-selections
echo "univention-kernel-image-2.6.26 hold" | dpkg --set-selections
```

- Die AVM-Kernel-Module wurde für den 2.6.26er Kernel sowohl für amd64 als auch für i386 gebaut (Bug 12910).
- Die FSC-Serverview-Module stehen für Kernel 2.6.18 zur Verfügung. Zusätzlich wurden für Kernel 2.6.26 die Kernel-Module angepasst und gebaut. Diese werden aber nicht offiziell von FSC unterstützt. Sobald FSC offizielle Module für Kernel 2.6.26 bereitstellt, wird Univention die Integration prüfen (Bug 12911).
- Für die amd64-Architektur werden keine 64GB (bigmem) Kernel-Meta-Pakete mehr gebaut. Wurden diese Pakete vor UCS 2.2 verwendet, so sollten die Meta-Pakete ohne 64GB-Erweiterung manuell installiert werden, bspw. **univention-kernel-image-2.6.18** oder **univention-kernel-image-2.6.26** (Bug 11839).

- Beim 2.6.18er Xen-Kernel ist nun auch die Kernel-Option **CONFIG_XEN_BLKDEV_TAP** gesetzt (Bug 12593).
- Beim Erzeugen der Ramdisk (update-initramfs) traten teilweise Fehlermeldungen auf, dass die `/boot`-Partition nur lesend eingebunden ist. Diese fehlerhafte Erkennung wurde korrigiert (Bug 13748).

10 Xen

- Xen wurde auf Version 3.2.1 aktualisiert (Bug 12866).
- Neben dem 2.6.18er Kernel ist nun auch der aktuellere UCS-Kernel 2.6.26 mit Xen Dom0-Unterstützung gebaut (Bug 12908).
- Das Paket **univention-xen** hat nun keine Abhängigkeit mehr auf den nicht PAE (Physical Address Extension) Hypervisor. Für den PAE-Hypervisor wird ein angepasster Kernel benötigt (Bug 13432).
- Die Xen-Beispielkonfigurationen wurden überarbeitet (Bug 10135).
- Xen Dom0-Systeme werden jetzt immer mit der Kernel Option **fbcon=map:2** gestartet, wodurch der Framebuffer deaktiviert wird (Bug 13432).
- Die Firmware-Pakete **firmware-bnx2**, **firmware-ipw2x00**, **firmware-iwlwifi**, **firmware-qlogic** und **firmware-ralink** wurden für UCS 2.2 gebaut (Bug 11965).

11 Univention Installer

- Die Prüfung des Rechner- bzw. Domänennamens im Installer wurden angepasst. Es sind nur Buchstaben und Zahlen und Bindestriche erlaubt. Am Anfang muss ein Buchstabe stehen, am Anfang und am Ende dürfen keine Bindestriche stehen (Bug 12646).
- Falls der Installer keine Netzwerkkarte findet, bekommt man nun eine entsprechende Warnung. Wird die Installation ohne funktionierende Netzwerkkarte fortgesetzt, wird während der Installation automatisch ein virtuelles Dummy-Netzwerkinterface eingerichtet, um die Installation erfolgreich abschließen zu können. Zusätzlich wird das Metapaket **firmware-all** installiert, wodurch diverse Firmwares für unterschiedliche Netzwerkkarten nach der Installation bereitstehen. Nähere Information können der Univention Support Datenbank entnommen werden (Bug 12427).
- Die Kernel-Module, die dem Installer mit der Option **loadmodules** übergeben werden, werden nun zu Beginn der Installation automatisch geladen (Bug 11276).
- Die Erstellung der Datei `/etc/fstab` wurde optimiert. Für CDROM- und DVD-Laufwerke werden jetzt die `/dev/cdrom*`-Geräte-Dateien verwendet (Bug 13681).
- Während der Installation wird das Installations-Profil nun vor dem Joinen des Systems bereitgestellt (Bug 10427).

- Am Ende der Installation werden nun einige Tests auf dem installierten System ausgeführt. Der Status der Installation wird angezeigt (Bug 12190).
- Über einen weiteren Punkt im Boot-Loader-Menü kann man nun die Installation im Software-Raid-Modus starten (Bug 13183).
- Die englische Übersetzung des Univention Installers und der System-Setup-Werkzeuge wurde überarbeitet (Bug 13326)
- Durch einen Fehler, der bei der profilbasierten Installation unter Verwendung eines AMD64-Installationsmediums auftrat, konnte keine Partitionierung der Festplatte durchgeführt werden. Dieser Fehler wurde jetzt behoben (Bug 11093).
- Das Passwort des Benutzers root wird jetzt während der Installation mit dem MD5-Hash-Verfahren verschlüsselt (Bug 9739).
- Wird die Installation über den Punkt Software-Raid im Boot-Menü gestartet, werden jetzt Kernel-Module für Software-Raid automatisch geladen (Bug 13197).
- Auf der Installations-DVD sind mit **mdadm** und **cfdisk** zwei weitere Tools zur Partitionierung installiert (Bug 13198)
- Falls der händische Partitionierungsmodus gewählt wurde, können die einzubindenden Partitionen während der Installation per Univention Configuration Registry-Variablen den Installations-Skripten bekannt gemacht werden (Bug 13204).
- Die Partitionierung bei einer profilbasierten Installation im Software-Raid-Modus kann über ein Shell-Skript erfolgen. Dies muss ein Skript mit dem Namen **01_partition.sh** im Verzeichnis **/script/installer** auf dem Installationsmedium untergebracht sein. Weitere Informationen sind im Handbuch zu finden (13202).
- Das Backup-Programm **bacula** kann nun im UCS Installer für die Installation ausgewählt werden (Bug 11885).
- Im Boot-Menü der Installations-DVD wurden die Einträge für **acpi=off** und **pci=noacpi** entfernt (Bug 13484).
- Während der Installation auf einem DC Master wird vor dem Generieren der Zertifikats-Infrastruktur versucht, die lokale Systemzeit mit time.fu-berlin.de abzugleichen. Andernfalls kann es sein, dass die Zertifikate nach dem Abgleich der Systemzeit noch nicht gültig sind (Bug 13549).

12 Univention Printserver

- Beim Anlegen von Druckern konnte ein nicht funktionierender Rechner-Account zu einer Endlosschleife führen. Diese mögliche Endlosschleife wird nun abgefangen (Bug 12777).
- Falls beim Anlegen eines Druckers der Drucker-Dienst (**cupsys**) nicht gestartet ist oder das Anlegen aus einem anderen Grund fehlschlägt, so wird ab sofort das Kommando zum Anlegen des Druckers zwischengespeichert und beim nächsten Start des Drucker-Dienstes automatisch erneut ausgeführt (Bug 9991).

- Auf dem lokalen Druckerserver wird jetzt die Univention Configuration Registry-Variablen **cups/printserver** auf **yes** gesetzt. Dadurch wird verhindert, dass auch auf dem lokalen Druckserver über eine Verzeichnisdienst-Richtlinie ein anderer Druckserver als der lokale eingetragen wird. Falls die Richtlinie Vorzug erhalten soll, so kann die Variable auf **no** gesetzt werden (Bug 10124).
- Falls während der Aktualisierung der Druck-Dienst **cupsys** nicht gestartet werden kann, so bricht die Aktualisierung nicht mehr ab. Dies ist notwendig, damit die Thin Client-Umgebung problemlos aktualisiert werden kann (Bug 13399).
- Die HP-Drucker-Treiber aus dem Paket **hplip** wurden aktualisiert. Während des Updates werden die neuen PPD-Dateien auch im Verzeichnisdienst referenziert, sobald das Join-Skript des Printerservers ausgeführt wurde. Dies geschieht auf den Systemrollen DC Master und DC Backup automatisch. Auf den anderen Systemrollen kann das Kommando **univention-run-join-scripts** ausgeführt werden. Durch Setzen der UCR-Variablen **cups/keep/ppds** auf **true** wird das automatische Ändern der PPD-Einträge im Verzeichnisdienst verhindert (Bug 13135).
- Die im Univention Directory Manager für CUPS-Druckerfreigaben vergebenen Berechtigungen werden jetzt auch von Samba ausgewertet und umgesetzt (Bugs 12086, 12043).
- Das neue Paket **univention-printserver-pdf** bietet die Möglichkeit, auf UCS-Printservern einen PDF-Drucker einzurichten, der Druckaufträge von Windows- oder Linux-Clients als PDF im Heimatverzeichnis des betreffenden Benutzers abspeichert (Bug 12235, 12165, 7625).

13 Weitere Dienste und Pakete

- Eine Kopie der GNU Public License in der neuen Version 3 ist unter `/usr/share/common-licenses/GPL-3` einsehbar (Bug 13374). Unter anderem macht die aktuelle Version des Pakets Samba von der neuen Lizenz Gebrauch.
- Berechtigungsprobleme mit dem Bind-Mount `/dev/.static/dev` in Verbindung mit Kernel 2.6.26 oder neuer wurden behoben (Bug 13751).
- Ein fehlender Symlink zu i386-Bibliotheken konnte auf amd64-Systemen zu Fehlermeldungen und Abstürzen von Dritthersteller-Produkten führen (Bug 11632).
- Das Tool **univention-share-replication** kann jetzt auch auf einem DC Slave ausgeführt werden (Bug 12320).
- Das Paket **univention-ssh** hat jetzt eine Abhängigkeit auf das Paket OpenSSH-Client Paket (Bug 12404).
- Während einer früheren Installation wurden die Gruppen (`scanner`, `nvrnm`, `rdma`, `fuse`, `kvm`) und der Benutzer `tss` nicht als Systemgruppen bzw. Systembenutzer angelegt. Dies konnte zu Überschneidungen zwischen den Benutzern und Gruppen im Verzeichnisdienst und den lokalen Benutzern und Gruppen führen. Während der Aktualisierung werden die Benutzer und Gruppen automatisch umgewandelt (Bug 13153).

- Der Timeout bei einer Plugin-Abfrage per NRPE kann ab sofort über Univention Configuration Registry konfiguriert werden, (`nagios/plugin/check_nrpe/timeout`) (Bug 13002).
- Der LDAP-Notifier wurde im Skript `preinst` während des Updates gestoppt, wodurch er nach dem Update nicht lief. Ab sofort wird der LDAP-Notifier nur noch im Skript `postinst` neu gestartet (Bug 13065).
- Ein `double free` in der C-Bibliothek von `univention-policy` wurde beseitigt (Bug 11460).
- In einigen Fällen hat der Kerberos-Passwortänderungsdienst (`kpasswd`) fälschlicherweise gemeldet, dass das Passwort erfolgreich geändert wurde, obwohl es zu kurz war. Dieses Problem wurde behoben (Bug 10013).
- Das Startskript des Domain Name Server **`bind9`** wird jetzt durch das Paket **`univention-bind-proxy`** zuverlässig ersetzt (Bug 12521).
- Das Hinzufügen eines Netzwerk-Interfaces über Univention System Setup konnte zu einer fehlerhaften Bind-Konfiguration führen. Dieser Fehler wurde behoben (Bug 9191).
- Mit Univention System Setup konnten die Netzwerkschnittstellen auf einem Managed- oder Mobileclient nicht auf DHCP umgestellt werden. Dieser Fehler wurde behoben. Zusätzlich wird dies nun auch in der Schnittstellenübersicht angezeigt (Bug 11798).
- Auf UCS-Systemen wird in der SSH-Konfiguration nun automatisch angepasst, wenn die Kerberos-Authentifizierung im PAM-Stack `de-/`aktiviert wird. Auf Mobileclient-Systemen werden so längere Wartezeiten bei einem SSH-Login vermieden, wenn der zuständige KDC nicht erreichbar ist (Bug 11127).
- Das Paket **`libapache2-mod-auth-ntlm-winbind`** wurde für UCS 2.2 neu gebaut. Mit diesem Apache-Modul kann die Anmeldung am Apache über NTLM/Winbind durchgeführt werden, wodurch ein Single-Sign-On von Windows-Systemen möglich ist (Bug 12935).
- Das Programm **`ldapvi`** wurde in die Distribution aufgenommen. Damit können sehr einfach Objekte im LDAP über die Kommandozeile modifiziert werden (Bug 13331).
- Das Paket **`univention-autofs`** wurde zur Distribution hinzugefügt. Die Konfiguration der `autofs`-Freigaben erfolgt dabei per Univention Configuration Registry (Bug 10586).
- Das Paket **`univention-fetchmail`** wurde hinzugefügt. Nach der Installation können im Univention Directory Manager für die Benutzer Fetchmail-Einstellungen vorgenommen (Bug 12384).
- 2009 wurde in die Liste der Copyright-Jahre aufgenommen (Bug 6875).

14 Sicherheitsupdates

- OpenOffice.org (CVE-2007-5745 CVE-2007-5746 CVE-2007-5747 CVE-2008-0320)

Mehrere Sicherheitslücken wurden in OpenOffice.org gefunden:

- Mehrere Pufferüberläufe beim Einlesen von Quattro Pro-Dateien erlauben das Ausführen von Code (CVE-2007-5745 CVE-2007-5747)
- Ein Pufferüberlauf beim Einlesen von EMF-Dateien erlaubt das Ausführen von Code (CVE-2007-5746)
- Ein Pufferüberlauf in der Verarbeitung von OLE-Dateien erlaubt das Ausführen von Code (CVE-2008-0320)

Dieses Update beseitigt alle diese Sicherheitslücken.

- Linux Kernel (CVE-2006-7051 CVE-2007-6282 CVE-2007-6716 CVE-2008-0598 CVE-2008-1514 CVE-2008-1673 CVE-2008-2729 CVE-2008-2812 CVE-2008-2826 CVE-2008-2931 CVE-2008-3272 CVE-2008-3275 CVE-2008-3276 CVE-2008-3525 CVE-2008-3833 CVE-2008-4210 CVE-2008-4302)

Lokale Nutzer können Posix-Timer allozieren und dadurch sämtlichen Arbeitsspeicher verbrauchen, was zur Terminierung von Prozessen führt. Diese Sicherheitslücke (CVE-2006-7051) kann durch das Beschränken der maximal zulässigen Signale pro Nutzer geschlossen werden — dies ist mit dem Befehl `ulimit -i` möglich.

- IPSEC DoS (CVE-2007-6282)
- DoS im dio-subsystem (CVE-2007-6716)
- Verwundbarkeit in der 32- und 64-Bit-Emulation (CVE-2008-0598)
- Über die ptrace-Testsuite kann ein Kernel Panic auf s390-Maschinen ausgelöst werden (CVE-2008-1514)
- ASN.1 BER-Daten werden nicht korrekt auf ihre Länge geprüft, so dass ein Crash ausgelöst, oder Code ausgeführt werden kann (CVE-2008-1673)
- Auf Amd64-System wird der Speicher nicht korrekt gelöscht, bevor er einem Programm zur Verfügung gestellt wird, so dass sensible Daten von Unbefugten zugegriffen werden könnten (CVE-2008-2729)
- Fehler NULL-Pointer-Checks im TTY-Handling können zu lokaler Privilege Escalation führen (CVE-2008-2812)
- Integerüberlauf in der `sctp_getsockopt_local_addrs_old`-Funktion führt zu einem Denial of Service (CVE-2008-2826)
- Privilege Escalation im Namespace-Code (CVE-2008-2931)
- Eine fehlerhafte Überprüfung der Device-Nummer in der Funktion `snd_seq_oss_synth_make_info` kann genutzt werden, um sensible Daten zuzugreifen (CVE-2008-3272)
- `real_lookup()` und `__lookup_hash()` DoS (CVE-2008-3275)
- Integerüberlauf in der `dccp_setsockopt_change`-Funktion ermöglicht es entfernten Angreifern einen Kernel Panic auszulösen (CVE-2008-3276)
- Die Funktion `sbni_ioctl` enthält einen Fehler in der Rechteüberprüfung, so dass Nutzer diese ausweiten können (CVE-2008-3525)

- Die Funktion `generic_file_splice_write` parsiert Nutzer- und Gruppen-IDs nicht korrekt, so dass ein Angreifer zusätzliche Gruppenrechte erlangen kann (CVE-2008-3833)
 - Die Funktion `generic_file_splice_write` parsiert Nutzer- und Gruppen-IDs nicht korrekt, so dass ein Angreifer zusätzliche Gruppenrechte erlangen kann – dies ist eine weitere Lücke, die unabhängig von CVE-2008-3833 ist (CVE-2008-4210)
 - Ein Fehler in der Funktion `add_to_page_cache_lru` führt dazu, dass ein System Crash verursacht wird (CVE-2008-4302)
- Xorg-X11 (CVE-2008-1377 CVE-2008-1379 CVE-2008-2360 CVE-2008-2361 CVE-2008-2362)

Mehrere Sicherheitslücken wurden im X-Server gefunden:

- Memory Corruption in der **Record and Security**-Erweiterung (CVE-2008-1377)
- Integerüberläufe in der MIT-SHM-Erweiterung können zum Auslesen von fremden Speichersegmenten ausgenutzt werden (CVE-2008-1379)
- Pufferüberlauf in der Render-Erweiterung (CVE-2008-2360)
- Integerüberläufe in der Render-Erweiterung (CVE-2008-2361)
- Integerüberläufe in der Render-Erweiterung (CVE-2008-2362)

Dieses Update beseitigt alle diese Sicherheitslücken.

- PHP5 (CVE-2007-3806 CVE-2008-1384 CVE-2008-2050 CVE-2008-2051 CVE-2008-2107 CVE-2008-2108 CVE-2007-5898)

Mehrere Sicherheitslücken wurden in PHP gefunden:

- `glob`-Funktion enthält Denial of Service-Schwäche, die evtl. auch zur Ausführung von Code ausgenutzt werden kann (CVE-2007-3806)
- Pufferüberlauf/NULL-Pointer-Deferenzierung in `fast-cgi` (CVE-2008-0599)
- Integerüberlauf in `printf`-Funktion (CVE-2008-1384)
- Pufferüberlauf in `fastcgi` (hier ist nicht unklar, inwiefern hier eine Sicherheitslücke vorliegt, oder ob die Daten alle aus vertrauenswürdiger Quelle kommen) (CVE-2008-2050)
- Der `GENERATE_SEED`-Macro erzeugt eine Reihe von 0-Bits, statt etwas zufälligem (CVE-2008-2107 CVE-2008-2108)
- Multibyte-Zeichen werden von `escapeshellcmd()` nicht escapet (CVE-2008-2051)
- Multibyte-Zeichen werden unsauber verarbeitet (CVE-2007-5898)

Dieses Update beseitigt alle diese Sicherheitslücken.

- MySQL-Server-5.0 (CVE-2007-2583 CVE-2007-2691 CVE-2007-2692 CVE-2007-3780 CVE-2007-3781 CVE-2007-3782 CVE-2007-5925 CVE-2007-5969 CVE-2007-6304 CVE-2008-0226 CVE-2008-0227 CVE-2008-2079 CVE-2008-3963)

Mehrere Sicherheitslücken wurden in der MySQL-Datenbank gefunden:

- Durch eine bestimmte IF-Abfrage kann der MySQL-Daemon zum Absturz gebracht werden (CVE-2007-2583)

- Zugriffsrechte für Tabellen wurden unzureichend geprüft, so dass Angreifer Tabellen umbenennen können (CVE-2007-2691)
- Die `mysql_change_db()`-Funktion setzt Zugriffsrechte inkorrekt zurück, wodurch Privilegien ausgeweitet werden können (CVE-2007-2692)
- Präparierte Passwort-Pakete können zu einem Absturz des MySQL-Daemons führen (CVE-2007-3780)
- Keine Rechteprüfung für SELECT-Statements mit LIKE-Option (CVE-2007-3781)
- Registrierte Nutzer können UPDATE-Privilegien auf Tabellen in anderen Datenbanken erlangen (CVE-2007-3782)
- Die `convert_search_mode_to_innabase`-Funktion kann zu einem Absturz des MySQL-Daemons führen (CVE-2007-5925)
- Verwendet eine Tabelle Symlinks, so können diese ausgenutzt werden, um den Symlink auf Systemdateien zu ändern (CVE-2007-5969)
- Über ein präpariertes SHOW-Statement kann der MySQL-Daemon zum Absturz (CVE-2007-6304)
- Pufferüberläufe in yaSSL erlauben Code-Ausführung (CVE-2008-0226)
- yaSSL kann über ein Hello-Paket Zugriffsrechte erlangen oder den MySQL-Daemon zum Absturz bringen (CVE-2008-0227)
- Zugriffsbeschränkungen für MyISAM-Tabellen können umgangen werden (CVE-2008-2079)
- Der MySQL-Daemon stürzt bei der Verarbeitung des leeren Bit-Strings ab (CVE-2008-3963)
- Zugriffsberechtigungen können für einige CREATE TABLE Befehle umgangen werden (CVE-2008-4097)

Dieses Update beseitigt alle diese Sicherheitslücken.

- rdesktop (CVE-2008-1801 CVE-2008-1802 CVE-2008-1803)

Mehrere Sicherheitslücken wurden im RDP-Client rdesktop gefunden:

- Ein Integerunderflow erlaubt das Ausführen von Code. (CVE-2008-1801)
- Ein Pufferüberlauf erlaubt das Ausführen von Code (CVE-2008-1802)
- Ein Integerüberlauf erlaubt das Ausführen von Code (CVE-2008-1803)

Dieses Update beseitigt alle diese Sicherheitslücken.

- Adobe Reader (CVE-2008-0655 CVE-2008-0667 CVE-2008-0726)

Mehrere Sicherheitslücken wurden im PDF-Viewer Adobe Reader gefunden:

- Mehrere unspezifizierte Lücken mit unbekanntem Auswirkungen (CVE-2008-0665)
- Dokumente können ohne Nutzerinteraktion ausgedruckt werden (CVE-2008-0667)
- Ein Integerüberlauf, der das Ausführen von Code ermöglicht (CVE-2008-0726)

Dieses Update beseitigt alle diese Sicherheitslücken.

- Java (CVE-2008-3115 CVE-2008-3114 CVE-2008-3113 CVE-2008-3112 CVE-2008-3111 CVE-2008-3110 CVE-2008-3109 CVE-2008-3108 CVE-2008-3107 CVE-2008-3106 CVE-2008-3105 CVE-2008-3104 CVE-2008-3103)

Java wurde auf die Version 1.5.0-16-3 aktualisiert, die die folgenden Lücken behebt:

- Secure Static Versioning von Java-Applets funktioniert nicht. (CVE-2008-3115)
 - Die Position des Caches kann von Applikationen ausgelesen werden. (CVE-2008-3114)
 - Eine Sicherheitslücke in Web Start erlaubt Applikationen Dateien zu erzeugen oder zu entfernen. (CVE-2008-3113)
 - Eine Sicherheitslücke in Web Start erlaubt Applikationen Dateien zu erzeugen oder zu entfernen. (CVE-2008-3112)
 - Pufferüberläufe erlauben das Ausweiten von Privilegien. (CVE-2008-3111)
 - Ein Fehler im Scripting erlaubt das Auslesen von Informationen anderer Applets. (CVE-2008-3110)
 - Ein Fehler im Scripting erlaubt das Ausweiten von Privilegien. (CVE-2008-3109)
 - Ein Pufferüberlauf im Auslesen von Schriften erlaubt das Ausweiten von Rechten. (CVE-2008-3108)
 - Ein Fehler in der virtuellen Maschine erlaubt das Ausweiten von Rechten. (CVE-2008-3107)
 - Ein Fehler im XML-Parser erlaubt Information Disclosure. (CVE-2008-3106)
 - Ein Fehler in JAX-WS erlaubt Information Disclosure. (CVE-2008-3105)
 - Fehler im Security-Modell erlaubt den Zugriff auf lokale Daten. (CVE-2008-3104)
 - Ein Fehler im Monitoring erlaubt das Ausweiten von Rechten. (CVE-2008-3103)
- Openldap2.3 (CVE-2007-5707 CVE-2007-5708 CVE-2007-6698 CVE-2008-0658 CVE-2008-2952)

Mehrere Sicherheitslücken wurden in OpenLDAP gefunden:

- slapd kann durch ein manipuliertes modify zum Crash gebracht werden. (CVE-2007-5707)
- slapo-pcache kann durch bestimmte Suchanfragen zum Crash gebracht werden. (CVE-2007-5708)
- Ein Fehler in der Anbindung von BDB erlaubt den slapd durch bestimmte modify-Anfragen zum Crash zu bringen. (CVE-2007-6698)
- Ein Fehler in der Anbindung von BDB erlaubt den slapd durch bestimmte modrdn-Anfragen zum Crash zu bringen. (CVE-2008-0658)
- Server-Absturz durch ein präpariertes ASN.1 BER-Paket. (CVE-2008-2952)

Dieses Update beseitigt alle diese Sicherheitslücken.

- Horde (CVE-2008-1284 CVE-2008-3823 CVE-2008-3824)

Mehrere Sicherheitslücken wurden in Horde gefunden:

- Remote File Inclusion in der Theme-Auswahl (CVE-2008-1284)

- MIME-Bibliothek erzeugt Text-Ausgaben, die vom Webbrowser interpretiert werden (CVE-2008-3823)
- Cross-Site-Scripting-Probleme mit HTML-Mails (CVE-2008-3824)

Dieses Update beseitigt alle diese Sicherheitslücken.

- Turba (CVE-2008-0807) Die Horde-Kontaktverwaltung Turba führt unzureichende Berechtigungs-Prüfungen im Bearbeiten von Adressen aus. Dieses Update beseitigt diese Sicherheitslücke.
- Firefox (CVE-2008-2785 CVE-2008-2933 CVE-2008-2934 CVE-2008-3837 CVE-2008-4058 CVE-2008-4060 CVE-2008-4061 CVE-2008-4062 CVE-2008-4063 CVE-2008-4064 CVE-2008-4065 CVE-2008-4066 CVE-2008-4067, CVE-2008-5012, CVE-2008-5013, CVE-2008-5014, CVE-2008-5015, CVE-2008-5016, CVE-2008-5017, CVE-2008-5018, CVE-2008-5019, CVE-2008-0017, CVE-2008-5021, CVE-2008-5022, CVE-2008-5023, CVE-2008-5024, CVE-2008-5513, CVE-2008-5512, CVE-2008-5511, CVE-2008-5510, CVE-2008-5508, CVE-2008-5507, CVE-2008-5506, CVE-2008-5505, CVE-2008-5502, CVE-2008-5500, CVE-2008-5501)

Firefox wurde auf Version 3.0.6 aktualisiert, die folgende Sicherheitslücken beseitigt:

- Ein Integer-Überlauf in einer Referenz auf die CSSValue-Datenstruktur ermöglicht die Ausführung von beliebigem Code durch einen entfernten Angreifer (CVE-2008-2785)
- Das Pipe-Zeichen (|) wird in einem URI als Anfrage zum Öffnen von Tabs interpretiert, was ein Angreifer ausnutzen kann, um beliebige lokale Dateien auszu-lesen (CVE-2008-2933)
- Eine präparierte GIF-Datei kann zum Absturz von Firefox und zur Ausführung von Code genutzt werden. (CVE-2008-2934)
- Fenster-Manipulationen können zu ungewollten Drag-and-Drop-Events führen (CVE-2008-3837) (CVE-2008-4058)
- Privilege Escalation auf Chrome-Level in XSLT-Handler (CVE-2008-4060)
- Crashes in der Layout-Engine erlauben das Ausführen von Code (CVE-2008-4061)
- Crashes in der Javascript-Engine erlauben das Ausführen von Code (CVE-2008-4062)
- Crashes in der Layout-Engine erlauben das Ausführen von Code (CVE-2008-4063)
- Crashes in der Grafik-Rendering-Engine erlauben das Ausführen von Code (CVE-2008-4064)
- Unicode Byte Order Marks werden aus Javascript entfernt, was zu Problemen führen kann wenn gequotete Strings als Code ausgeführt werden (CVE-2008-4065)
- Unicode Ersatzzeichen (Surrogates) werden vom HTML-Parser ignoriert (CVE-2008-4066)
- resource:-URLs können zu Directory-Traversal führen (CVE-2008-4067)
- resource:-URLs können lokale Beschränkungen umgehen (CVE-2008-4068)

- Same-Origin-Prüfungen können umgangen werden, was zu Information Disclosure führen kann (CVE-2008-5012)
 - Durch eine fehlende Fehlerbehandlung bei der Einbindung des Flash-Plugins kann potentiell Code ausgeführt werden. (CVE-2008-5013)
 - Fehlerhaftes Locking von internen Firefox-Objekten kann zum Ausführen von Code führen. (CVE-2008-5014)
 - Chrome Privilege Escalation bei einigen URI-Typen. (CVE-2008-5015)
 - Crashes in der Layout- und der Javascript-Engine können zum Ausführen von Code führen. (CVE-2008-5016, CVE-2008-5017, CVE-2008-5018)
 - Same-Origin-Prüfungen können umgangen werden, was zu Privilege Escalation führen kann. (CVE-2008-5019)
 - Ein Fehler im MIME-Parser kann zum Ausführen von Code führen. (CVE-2008-0017)
 - Ein Fehler im DOM-Parser kann zum Ausführen von Code führen. (CVE-2008-5021)
 - Same-Origin-Prüfungen können umgangen werden, was zu Cross-Site-Scripting führen kann. (CVE-2008-5022)
 - Javascript kann in Jar-Archive eingeschleust werden. (CVE-2008-5023)
 - E4X-Dokumente werden inkorrekt geparkt. (CVE-2008-5024)
 - Durch das Session-Restore-Feature können Same-Origin-Prüfungen des Browsers umgangen werden. (CVE-2008-5513)
 - Zwei Fehler in XPCNativeWrappers erlauben das Ausweiten von Javascript-Rechten auf die Chrome-Rechte. (CVE-2008-5512)
 - Durch XBL-Bindings kann die Same-Origin-Policy des Browsers umgangen werden. (CVE-2008-5511)
 - Der CSS-Parser ignoriert escapede Null-Zeichenketten, was dazu führen kann, dass Eingabebereinigungsroutinen ausgehebelt werden können. (CVE-2008-5510)
 - Einige Steuerzeichen werden vom URL-Parser nicht korrekt erkannt. (CVE-2008-5508)
 - Ein Fehler in der DOM-API kann dazu führen, dass Informationen von anderen Webseiten gelesen werden können. (CVE-2008-5507)
 - Antworten auf weitergeleitete XMLHttpRequests können von fremden Seiten ausgelesen werden. (CVE-2008-5506)
 - Benutzer sind über das XUL-Attribut "persist" für Webseiten identifizierbar. (CVE-2008-5505)
 - Crashes in der Javascript-Engine erlauben potentiell das Ausführen von Code. (CVE-2008-5502)
 - Crashes in der Layout-Engine erlauben potentiell das Ausführen von Code. (CVE-2008-5500, CVE-2008-5501)
- Tiff-Bibliothek (CVE-2008-2327)

Mehrere Speicherunterläufe im LZW-Dekoder der Tiff-Bibliothek ermöglichen die Ausführung von Code durch präparierte TIFF-Dateien. Dieses Update beseitigt diese Sicherheitslücken.

- Python (CVE-2008-2315 CVE-2008-3142 CVE-2008-3143 CVE-2008-3144)

Mehrere Sicherheitslücken wurden im Python-Interpreter entdeckt:

- Mehrere Integer-Überläufe können von einem Angreifer ausgenutzt werden (CVE-2008-2315)
- Mehrere Pufferüberläufe ermöglichen es einem Angreifer den Python-Interpreter zum Absturz zu bringen (CVE-2008-3142)
- Mehrere Integer-Überläufe könnten es einem Angreifer ermöglichen beliebigen Code auszuführen (CVE-2008-3143)
- Weitere Integer-Überläufe ermöglichen einen Denial of Service-Angriff (CVE-2008-3144)

Dieses Update beseitigt alle diese Sicherheitslücken.

- Postfix (CVE-2008-2936)

Postfix behandelt einen symbolischen Link unsicher, was es einem lokalen Benutzer durch das Anhängen von Daten an eine Datei erlaubt potentiell Root-Rechte zu erlangen. Diese Sicherheitslücke wurde beseitigt.

- ClamAV (CVE-2008-1389 CVE-2008-3912 CVE-2008-3913 CVE-2008-3914)

Mehrere Sicherheitslücken wurden im Virens scanner ClamAV entdeckt:

- Sicherheitslücken im chm-Format-Parser, die zum Crash führen können (CVE-2008-1389)
- Denial of Service Angriff möglich auf libclamav (CVE-2008-3912)
- Denial of Service Angriff möglich, bei dem massiv Arbeitsspeicher von clamav angefordert wird (CVE-2008-3913)
- DoS durch Filedescriptor-Leak (CVE-2008-3914)

Dieses Update beseitigt diese Sicherheitslücken.

- Perl (CVE-2007-5116, CVE-2008-1927, CVE-2008-5302, CVE-2008-5303)

Mehrere Sicherheitslücken wurden im Interpreter für die Skriptsprache Perl gefunden, die zum Ausführen von Code, Denial of Service oder dem Ausweiten von Systemrechten führen können:

- Mehrere Bufferoverflows in der Verarbeitung von Unicode-Sequenzen in der Verarbeitung von regulären Ausdrücken. (CVE-2007-5116, CVE-2008-1927)
- Eine Race Condition in der rmtree()-Funktion des File::Path Moduls (CVE-2008-5302, CVE-2008-5303)

Dieses Update beseitigt alle diese Sicherheitslücken.