univention
be open.

Changelog for Univention Corporate Server (UCS) 5.0-8

Release 5.0-8

Jun 12, 2024

CONTENTS

CHAPTER

ONE

GENERAL

- UCS 5.0-8 includes all issued security updates issued for UCS 5.0-7:
  - **bind9** (CVE-2023-50387, CVE-2023-50868) (Bug #57301)
  - **bluez** (CVE-2023-27349) (Bug #57342)
  - **containerd** (CVE-2020-15257, CVE-2021-21334, CVE-2021-41103, CVE-2022-23471, CVE-2022-23648, CVE-2023-25153, CVE-2023-25173) (Bug #56457)
  - **curl** (CVE-2023-27534) (Bug #57160)
  - **docker.io** (CVE-2021-21284, CVE-2021-21285, CVE-2021-41089, CVE-2021-41091, CVE-2021-41092) (Bug #56457)
  - **emacs** (CVE-2024-30203, CVE-2024-30204, CVE-2024-30205) (Bug #57250)
  - **expat** (CVE-2023-52425) (Bug #57215)
  - **firefox-esr** (CVE-2023-5388, CVE-2024-0743, CVE-2024-2607, CVE-2024-2608, CVE-2024-2609, CVE-2024-2610, CVE-2024-2611, CVE-2024-2612, CVE-2024-2614, CVE-2024-2616, CVE-2024-29944, CVE-2024-3302, CVE-2024-3852, CVE-2024-3854, CVE-2024-3857, CVE-2024-3859, CVE-2024-3861, CVE-2024-3864, CVE-2024-4367, CVE-2024-4767, CVE-2024-4768, CVE-2024-4769, CVE-2024-4770, CVE-2024-4777) (Bug #57198, Bug #57232, Bug #57303)
  - **glib2.0** (CVE-2024-34397) (Bug #57300)
  - **glibc** (CVE-2024-2961) (Bug #57249)
  - **golang-1.13** (CVE-2020-16845, CVE-2022-1705, CVE-2022-27664, CVE-2022-28131, CVE-2022-2879, CVE-2022-2880, CVE-2022-30629, CVE-2022-30631, CVE-2022-30632, CVE-2022-30633, CVE-2022-30635, CVE-2022-32148, CVE-2022-32189, CVE-2022-41717, CVE-2023-24534, CVE-2023-24537, CVE-2023-24538) (Bug #56457)
  - **golang-1.18** (CVE-2020-16845, CVE-2022-1705, CVE-2022-1962, CVE-2022-27664, CVE-2022-28131, CVE-2022-2879, CVE-2022-2880, CVE-2022-29526, CVE-2022-30629, CVE-2022-30630, CVE-2022-30631, CVE-2022-30632, CVE-2022-30633, CVE-2022-30635, CVE-2022-32148, CVE-2022-32189, CVE-2022-41715, CVE-2022-41717, CVE-2023-24534, CVE-2023-24537, CVE-2023-24538) (Bug #56457)
  - **imagemagick** (CVE-2022-48541) (Bug #57176)
  - **intel-microcode** (CVE-2023-22655, CVE-2023-28746, CVE-2023-38575, CVE-2023-39368, CVE-2023-43490) (Bug #57252)
  - **libgd2** (CVE-2018-14553, CVE-2021-38115, CVE-2021-40812) (Bug #57216)
  - **libnet-cidr-lite-perl** (CVE-2021-47154) (Bug #57179)
  - **libvirt** (CVE-2020-10703, CVE-2020-12430, CVE-2020-25637, CVE-2021-3631, CVE-2021-3667, CVE-2021-3975, CVE-2021-4147, CVE-2022-0897, CVE-2024-1441, CVE-2024-2494, CVE-2024-2496) (Bug #57199)
  - **nghttp2** (CVE-2024-28182) (Bug #57251)

- **nss** (CVE-2023-5388, CVE-2024-0743) (Bug #57152)
- **openjdk-11** (CVE-2024-21011, CVE-2024-21012, CVE-2024-21068, CVE-2024-21085, CVE-2024-21094) (Bug #57234)
- **php7.3** (CVE-2022-31629, CVE-2023-3823, CVE-2024-2756, CVE-2024-3096) (Bug #57270)
- **pillow** (CVE-2021-23437, CVE-2022-22817, CVE-2023-44271, CVE-2024-28219) (Bug #57180, Bug #57225)
- **postgresql-11** (CVE-2024-0985) (Bug #57175)
- **python-idna** (CVE-2024-3651) (Bug #57272)
- **python2.7** (CVE-2024-0450) (Bug #57178)
- **python3.7** (CVE-2023-6597, CVE-2024-0450) (Bug #57177)
- **qemu** (CVE-2023-2861, CVE-2023-3354, CVE-2023-5088) (Bug #57149)
- **runc** (CVE-2021-30465, CVE-2023-25809, CVE-2023-27561, CVE-2023-28642, CVE-2024-21626) (Bug #56457)
- **shim** (CVE-2024-2312) (Bug #57271)
- **tar** (CVE-2023-39804) (Bug #57150)
- **tiff** (CVE-2023-3576, CVE-2023-52356) (Bug #57151)
- **util-linux** (CVE-2021-37600, CVE-2024-28085) (Bug #57214)
- **xorg-server** (CVE-2024-31080, CVE-2024-31081, CVE-2024-31083) (Bug #57224)

- UCS 5.0-8 includes the following updated packages from Debian 10.13:

  cacti, **composer**, **distro-info-data**, **fossil**, **freeipa**, **frr**, **gross**, **gst-plugins-base1.0**, **gtkwave**, **jetty9**, **knot-resolver**, **less**, **libcaca**, **libdate-time-timezone-perl**, **libkf5ksieve**, **libpgjava**, **mediawiki**, **nodejs**, **node-xml2js**, **org-mode**, **putty**, **python-pymysql**, **qtbase-opensource-src**, **ruby-rack**, **shim-helpers-amd64-signed**, **trafficserver**, **tzdata**, **unadf**, **zfs-linux**

- UCS 5.0-8 includes the following packages in the maintained repository of UCS:

  crudeoauth

CHAPTER

TWO

DOMAIN SERVICES

- Fix dependency of server role packages to explicitly depend on a fixed version of Univention Configuration Registry. This fixes a regression caused by erratum 988 (Bug #57132).

2.1 LDAP Directory Manager

- Adjusted Univention Directory Manager to support declaring properties as lazy loading. If a property is lazy loading, UCS only fetches it, if explicitly requested. Added the flag `--properties` to Univention Directory Manager CLI to request specific properties (Bug #57110).
- If the Univention Configuration Registry Variable `directory/manager/mail-address/uniqueness` has the value `true`, the uniqueness check for email addresses takes both user properties, `mailPrimaryAddress` and `mailAlternativeAddress`, into account. It's now possible to swap the values for these properties with one change to the user object (Bug #57171).
- Updated the Univention Directory Manager module `settings/extended_attributes` to include the property `preventUmcDefaultPopup` which UCS evaluates in the Univention Management Console. It inhibits UCS from warning the user that a modification sets the default value of a property (Bug #51187).
- Addressed a regression impacting the modification of `users/ldap` objects within the Univention Management Console, stemming from erratum 1018 (Bug #57228).
- Restored compatibility with Python 2.7, which erratum 991 has broken (Bug #57146).
- Added ability to filter for various attributes using the Univention Directory Manager command line interface and in Univention Management Console. This includes `sambaLogonHours` and `accountActivationDate` for the `users/user` module, `hwaddress` for the `dhcp/host` module and `ip` for the `dns/ptr_record` module (Bug #54339, Bug #54339, Bug #53830, Bug #54339, Bug #53830, Bug #53807, Bug #54339, Bug #53830, Bug #53807, Bug #55604).
- Added an asynchronous UDM HTTP REST API client (Bug #56735).
- Administrators can specify a list of properties that UDM HTTP REST API should return. As a default behavior, UDM HTTP REST API returns all regular properties. UDM HTTP REST API only returns lazy loading properties, if explicitly requested (Bug #57110).
- Enhanced the LDAP overlay `slapd-sock` by adding `extendedresults` as a possible value to the `sockresps` configuration option. With that configuration, the overlay outputs a changed LDIF in the `RESULT` phase, including *LDAPControl* data for `PostReadControl` and `PreReadControl` collected during CRUD operations. The output format is similar to the one used by the LDAP overlay `auditlog` with an additional `control:` field (Bug #57267).
- Added the Univention Configuration Registry Variable `directory/manager/feature/prepostread` to configure `univention.uldap` to send *LDAPControls* `PostReadControl` and `PreReadControl` for the CRUD operations `add`, `modify`, `modrdn`, and `delete`. If UCS has this option activated, the *LDAPControls* instruct OpenLDAP to return all regular and operational attributes that are readable by the `binddn` before and after the change (Bug #57267).

- UCS now allows configuring the LDAP overlay `slapd-sock` for `sockresps extendedresults` through the Univention Configuration Registry Variable `ldap/overlay/sock`. If activated, it outputs LDAP changes including LDIF for CRUD operations, not for search. Additionally, the Univention Configuration Registry Variable `ldap/overlay/sock/sockops` allows activating `sockops add delete modify modrdn`.

  Please note that activating that second Univention Configuration Registry Variable causes the **`slapd`** process to wait for confirmation for CRUD events, see **`man slapd-sock`**. So, you mustn't activate it, unless there is a suitable process responding to the socket path `/var/lib/univention-ldap/slapd-sock/sock`. The purpose of these changes is to feed into the provisioning queue of Nubus (Bug #57267).

CHAPTER

THREE

UNIVENTION MANAGEMENT CONSOLE

3.1 Univention Management Console web interface

- When a user selects a different language inside the Univention Management Console, it didn't use the language inside the modules. For example, the server provides German, but a user selects English as their preferred language, the modules were still in German. Fixed it and Univention Management Console uses the same language everywhere (Bug #57192).

3.2 Univention Portal

- In the past the user wasn't able to unset their birthday inside the self service, because the input validation didn't detect a valid date according to the ISO-8601 standard. Users can unset their birthday again (Bug #57023).

3.3 Univention Management Console server

- Univention Management Console now also logs the reason for a failed LDAP connection for module processes (Bug #57311).
- The Univention Management Console SAML (Secure Authentication Markup Language) client is now updated in Keycloak on changes, for example when changing the Univention Configuration Registry Variable `umc/saml/assertion-lifetime` (Bug #57143).
- Fixed a memory leak in the Univention Management Console server (Bug #57104).
- Fixed a LDAP connection leak in the Univention Management Console server (Bug #57113).
- The permission and ownership of the Univention Management Console log file is now only modified if it isn't `STDOUT` or `STDERR` (Bug #57154).
- If the UCS primary directory node is on UCS version 5.2-0 or higher, Univention Management Console no longer creates or configures a client for `simpleSAMLphp` (Bug #57163).
- Added the option `copytruncate` to the **`logrotate`** configuration of Univention Management Console to not delete log files, but to truncate the original log file to zero size in place (Bug #56906).
- Added a missing Univention Configuration Registry Variable to the trigger the **`apache2`** `univention.conf` (Bug #57229).

3.4 Modules for system settings / setup wizard

- Adapted the Univention Management Console IP change module to check the zone of the single sign-n domain name case insensitively (Bug #57290).

3.5 System diagnostic module

- Added a diagnostic module to monitor the state of app queues (Bug #57217).

3.6 Policies

- `univention-policy` uses the `StartTLS` operation mode configured through the Univention Configuration Registry Variable `directory/manager/starttls` (Bug #57158, Bug #57173).
- `univention-policy` uses the LDAP port configured through the Univention Configuration Registry Variable `ldap/server/port` (Bug #57159, Bug #57173).
- Added a compiler flag to the building process to detect certain memory errors during the execution of **`univention_policy_result`** (Bug #57257).

3.7 LDAP directory browser

- The Univention Management Console Univention Directory Manager module fetches all lazy loading properties (Bug #57110).

CHAPTER

FOUR

UNIVENTION BASE LIBRARIES

- Added the LDAP schema attributes for the UCS authorization engine *Guardian* roles (Bug #57110).
- Even though all OCs inherit from top and **ldapsearch** actually finds them when searching for `(objectClass=top)`, the (inherited) `objectClass: top` doesn't show up as an attribute in the output of **ldapsearch** (Bug #50268).
- Updated the Univention Directory Manager module `settings/extended_attributes` to include the property `preventUmcDefaultPopup` which UCS evaluates in the Univention Management Console. It inhibits UCS from warning the user that a modification sets the default value of a property (Bug #51187).
- Erratum 991 improved the LDAP filters for DNS objects in Univention Directory Manager, but forgot to add an LDAP index for the `sOARecord` attribute there. This update fixes that and improves the performance of the Univention Management Console modules `computers` and `school computers`, especially for teachers in UCS@school environments, which are subject to a larger number of LDAP ACLs (Bug #57193).
- Added the helper functions `ucs_needsKeycloakSetup`, `ucs_needsSimplesamlphpSetup`, and `ucs_primaryVersionGreaterEqual` to easier evaluate what kind of SAML setup the domain needs (Bug #57163).

CHAPTER

FIVE

SYSTEM SERVICES

5.1 SAML

- Changed the LDAP filter for user objects in the LDAP federation configuration to require the attribute `uid` (Bug #57205).

5.2 RADIUS

- The RADIUS server now supports different MAC address formats for the MAB (MAC Authentication Bypass) feature (Bug #57069).
- The default enabled configuration under `/etc/freeradius/3.0/sites-enabled/` was reset to the default one during installation. This breaks setups with custom configurations (Bug #55007).

CHAPTER

SIX

OTHER CHANGES

- Newer version of package is required as build time dependency for **runc**, **containerd** and **docker.io** (Bug #56457).
- Fix Debian Bug #960887: `Use of uninitialized value $caller` (Bug #56457).
- Updated the following product logos: login page icon, `favicon`, portal icon, and Univention Management Console portal entry icon (Bug #57378).
- Added the GPG/PGP public key `univention-archive-key-ucs-52x.gpg` for UCS version 5.2. This key signs the UCS version 5.2 repository (Bug #57312).

INDEX

B

C

D

E

L

U