univention
be open.

Changelog for Univention Corporate Server (UCS) 5.0-6

Release 5.0-6

Dec 13, 2023

CONTENTS

1 General **1**
- 1.1 Univention Configuration Registry . . . 3
- 1.2 OpenLDAP . . . 3

2 Univention Management Console **5**
- 2.1 Univention Management Console web interface . . . 5
- 2.2 Univention Portal . . . 5
- 2.3 Univention Management Console server . . . 5
- 2.4 Univention App Center . . . 6
- 2.5 Univention Directory Manager and command line interface . . . 6
- 2.6 Modules for system settings / setup wizard . . . 6
- 2.7 Domain join module . . . 6
- 2.8 System diagnostic module . . . 6
- 2.9 File system quota module . . . 7

3 Univention base libraries **9**

4 Software deployment **11**

5 System services **13**
- 5.1 SAML . . . 13
- 5.2 Mail services . . . 13
- 5.3 SSL . . . 14
- 5.4 DHCP server . . . 14
- 5.5 PAM / Local group cache . . . 14

6 Services for Windows **15**
- 6.1 Samba . . . 15
- 6.2 Univention S4 Connector . . . 15
- 6.3 Univention Active Directory Connection . . . 16

Index **17**

CHAPTER

ONE

GENERAL

- All security updates issued for UCS 5.0-5 are included:
  - **c-ares** (CVE-2020-22217) (Bug #56608)
  - **cups** (CVE-2023-32360, CVE-2023-4504) (Bug #56679)
  - **curl** (CVE-2023-28321, CVE-2023-38546) (Bug #56745)
  - **dbus** (CVE-2023-34969) (Bug #56778)
  - **elfutils** (CVE-2020-21047) (Bug #56652)
  - **exim4** (CVE-2023-42114, CVE-2023-42116) (Bug #56706)
  - **firefox-esr** (CVE-2022-23597, CVE-2022-2505, CVE-2022-36315, CVE-2022-36316, CVE-2022-36318, CVE-2022-36319, CVE-2022-36320, CVE-2022-38472, CVE-2022-38473, CVE-2022-38475, CVE-2022-38477, CVE-2022-38478, CVE-2022-40674, CVE-2022-40956, CVE-2022-40957, CVE-2022-40958, CVE-2022-40959, CVE-2022-40960, CVE-2022-40962, CVE-2022-42927, CVE-2022-42928, CVE-2022-42929, CVE-2022-42930, CVE-2022-42931, CVE-2022-42932, CVE-2022-45403, CVE-2022-45404, CVE-2022-45405, CVE-2022-45406, CVE-2022-45407, CVE-2022-45408, CVE-2022-45409, CVE-2022-45410, CVE-2022-45411, CVE-2022-45412, CVE-2022-45415, CVE-2022-45416, CVE-2022-45417, CVE-2022-45418, CVE-2022-45419, CVE-2022-45420, CVE-2022-45421, CVE-2022-46871, CVE-2022-46872, CVE-2022-46873, CVE-2022-46874, CVE-2022-46877, CVE-2022-46878, CVE-2022-46879, CVE-2023-0767, CVE-2023-23598, CVE-2023-23601, CVE-2023-23602, CVE-2023-23603, CVE-2023-23604, CVE-2023-23605, CVE-2023-23606, CVE-2023-25728, CVE-2023-25729, CVE-2023-25730, CVE-2023-25731, CVE-2023-25732, CVE-2023-25733, CVE-2023-25735, CVE-2023-25736, CVE-2023-25737, CVE-2023-25739, CVE-2023-25741, CVE-2023-25742, CVE-2023-25744, CVE-2023-25745, CVE-2023-25750, CVE-2023-25751, CVE-2023-25752, CVE-2023-28160, CVE-2023-28161, CVE-2023-28162, CVE-2023-28164, CVE-2023-28176, CVE-2023-28177, CVE-2023-29533, CVE-2023-29535, CVE-2023-29536, CVE-2023-29537, CVE-2023-29538, CVE-2023-29539, CVE-2023-29540, CVE-2023-29541, CVE-2023-29543, CVE-2023-29544, CVE-2023-29547, CVE-2023-29548, CVE-2023-29549, CVE-2023-29550, CVE-2023-29551, CVE-2023-32205, CVE-2023-32206, CVE-2023-32207, CVE-2023-32208, CVE-2023-32209, CVE-2023-32210, CVE-2023-32211, CVE-2023-32212, CVE-2023-32213, CVE-2023-32215, CVE-2023-32216, CVE-2023-34414, CVE-2023-34415, CVE-2023-34416, CVE-2023-34417, CVE-2023-3482, CVE-2023-3600, CVE-2023-37201, CVE-2023-37202, CVE-2023-37203, CVE-2023-37204, CVE-2023-37205, CVE-2023-37206, CVE-2023-37207, CVE-2023-37208, CVE-2023-37209, CVE-2023-37210, CVE-2023-37211, CVE-2023-37212, CVE-2023-4045, CVE-2023-4046, CVE-2023-4047, CVE-2023-4048, CVE-2023-4049, CVE-2023-4050, CVE-2023-4051, CVE-2023-4053, CVE-2023-4055, CVE-2023-4056, CVE-2023-4057, CVE-2023-4573, CVE-2023-4574, CVE-2023-4575, CVE-2023-4577, CVE-2023-4578, CVE-2023-4580, CVE-2023-4581, CVE-2023-4583, CVE-2023-4584, CVE-2023-4585, CVE-2023-4863, CVE-2023-5169, CVE-2023-5171, CVE-2023-5176, CVE-2023-5217, CVE-2023-5721, CVE-2023-5724, CVE-2023-5725, CVE-2023-5728, CVE-2023-5730, CVE-2023-5732, CVE-2023-6204, CVE-2023-6205, CVE-2023-6206, CVE-2023-6207, CVE-2023-6208, CVE-2023-6209, CVE-2023-6212) (Bug #56607, Bug #56676, Bug #56780, Bug #56876)

- **firmware-nonfree** (CVE-2022-27635, CVE-2022-36351, CVE-2022-38076, CVE-2022-40964, CVE-2022-46329) (Bug #56683)
- **flac** (CVE-2020-22219) (Bug #56653)
- **ghostscript** (CVE-2020-21710, CVE-2020-21890) (Bug #56655)
- **glib2.0** (CVE-2023-29499, CVE-2023-32611, CVE-2023-32665) (Bug #56654)
- **gnutls28** (CVE-2023-5981) (Bug #56877)
- **grub-efi-amd64-signed** (CVE-2023-4692, CVE-2023-4693) (Bug #56742)
- **grub2** (CVE-2023-4692, CVE-2023-4693) (Bug #56742)
- **krb5** (CVE-2023-36054) (Bug #56755)
- **libde265** (CVE-2023-27102, CVE-2023-27103, CVE-2023-43887, CVE-2023-47471) (Bug #56892)
- **libwebp** (CVE-2023-4863) (Bug #56633)
- **libx11** (CVE-2023-43785, CVE-2023-43786, CVE-2023-43787) (Bug #56741)
- **libxpm** (CVE-2023-43788, CVE-2023-43789) (Bug #56744)
- **memcached** (CVE-2022-48571) (Bug #56738)
- **ncurses** (CVE-2020-19189, CVE-2021-39537, CVE-2023-29491) (Bug #56684, Bug #56893)
- **nghttp2** (CVE-2020-11080, CVE-2023-44487) (Bug #56740)
- **nss** (CVE-2020-25648, CVE-2023-4421) (Bug #56779)
- **openjdk-11** (CVE-2023-21930, CVE-2023-21937, CVE-2023-21938, CVE-2023-21939, CVE-2023-21954, CVE-2023-21967, CVE-2023-21968, CVE-2023-22006, CVE-2023-22036, CVE-2023-22041, CVE-2023-22045, CVE-2023-22049, CVE-2023-22081, CVE-2023-25193) (Bug #56632, Bug #56776)
- **poppler** (CVE-2020-23804, CVE-2022-37050, CVE-2022-37051) (Bug #56746)
- **postgresql-11** (CVE-2023-2454, CVE-2023-2455, CVE-2023-5868, CVE-2023-5869, CVE-2023-5870) (Bug #56677, Bug #56821)
- **python-reportlab** (CVE-2019-19450, CVE-2020-28463) (Bug #56678)
- **python-urllib3** (CVE-2018-20060, CVE-2018-25091, CVE-2019-11236, CVE-2019-11324, CVE-2020-26137, CVE-2023-43803, CVE-2023-43804) (Bug #56743, Bug #56822)
- **python2.7** (CVE-2021-23336, CVE-2022-0391, CVE-2022-48560, CVE-2022-48565, CVE-2022-48566, CVE-2023-24329, CVE-2023-40217) (Bug #56644)
- **python3.7** (CVE-2022-48560, CVE-2022-48564, CVE-2022-48565, CVE-2022-48566, CVE-2023-40217) (Bug #56739)
- **samba** (CVE-2023-3961, CVE-2023-4091, CVE-2023-4154, CVE-2023-42669, CVE-2023-42670) (Bug #56696)
- **univention-directory-listener** (CVE-2023-38994) (Bug #56354)
- **univention-directory-manager-modules** (CVE-2023-38994) (Bug #56354)
- **univention-directory-replication** (CVE-2023-38994) (Bug #56354)
- **univention-ldap** (CVE-2023-38994) (Bug #56333, Bug #56767)
- **univention-licence** (CVE-2023-38994) (Bug #56354)
- **univention-nagios** (CVE-2023-38994) (Bug #56354)
- **univention-samba** (CVE-2023-38994) (Bug #56332)
- **univention-samba4** (CVE-2023-38994) (Bug #56354)

  - **vim** (CVE-2023-4752, CVE-2023-4781) (Bug #56675)
  - **xorg-server** (CVE-2023-5367, CVE-2023-5380) (Bug #56777)

- The following updated packages from Debian 10.13 are included:

  activemq amanda asmtools audiofile axis batik cargo-mozilla ceph cryptojs distro-info distro-info-data e2guardian exempi freeimage freerdp2 frr gerbv gimp gimp-dds gnome-boxes gsl h2o horizon inetutils jetty9 jtreg6 libapache-mod-jk libclamunrar libcue libvpx libyang lldpd lwip minizip mutt netty node-babel node-browserify-sign node-cookiejar node-json5 opendkim org-mode orthanc phppgadmin pmix postgresql-multicorn prometheus-alertmanager python-requestbuilder qemu redis reportbug request-tracker4 roundcube ruby-loofah ruby-rails-html-sanitizer ruby-rmagick ruby-sanitize rust-cbindgen rustc-mozilla strongswan tang testng7 thunderbird tomcat9 trapperkeeper-webserver-jetty9-clojure vinagre vlc zbar zookeeper

- The following packages have been moved to the maintained repository of UCS:

  py-lmdb (Bug #53387)

- Execute the pre-installation script for server role Primary Directory Node with **bash**. This is needed to create the SSL/TLS certificate (Bug #56046).

1.1 Univention Configuration Registry

1.1.1 Changes to templates and modules

- The configuration file `/etc/selinux/config` has been added to disable SELinux. SELinux is not supported by UCS (Bug #56005).

1.2 OpenLDAP

1.2.1 Listener/Notifier domain replication

- Some new attributes that will be provided by OpenLDAPs **ppolicy** from version 2.5 on, were removed from the schema replication exclusion list, to allow interoperability with the new OpenLDAP version (Bug #56729).
- The script **univention-directory-replication** created a temporary password file with a newline in it, which therefore contained an invalid password. This resulted in **slapd** not being able to import a file `failed.ldif` on startup. This fixes a regression from UCS 5.0 erratum 870 (Bug #56801).

CHAPTER

TWO

UNIVENTION MANAGEMENT CONSOLE

2.1 Univention Management Console web interface

- The request header `If-Match` can now be given in `DELETE` requests to make them conditional (Bug #56731).
- Missing properties when creating or modifying objects are now correctly marked in the error response (Bug #56734).
- The unsupported HTML developer view of the UDM REST API has been disabled and can be enabled via the Univention Configuration Registry Variable `directory/manager/rest/html-view- enabled` (Bug #56714).
- Duplicate settings for the Keycloak app have been removed from the theme styles (Bug #56548).
- The error handling for progress bars has been improved so that Apache restarts during app installations don't cause failures anymore (Bug #56562).

2.2 Univention Portal

- The deletion of a user's profile picture via **`Self Service`** has been repaired (Bug #56349).
- The labels of the **`Self Service`** forms were always displayed in English when they were accessed directly via URL without navigating through the portal. They are now translated correctly (Bug #56660).
- Update file `portals.json` atomically to prevent inconsistent reading (Bug #53860).

2.3 Univention Management Console server

- The detection of active requests has been corrected so that module processes cannot be exited anymore if there are still open requests. This was broken since Bug #56198 UCS 5.0 erratum 721 (Bug #56575).
- The configured maximum request body size is now respected (Bug #56510).
- The maximum number of parallel HTTP connections from the UMC-Server to UMC module processes has been raised from 10 to unlimited (Bug #56828).
- User preferences (such as favorite Univention Management Console modules) could not be set via old UMC clients from UCS systems before UCS 5.0-3. The functionality has been restored (Bug #56753).
- Explicit defaults for cookie settings were added to `/var/www/univention/meta.json` so they are available for all components that needs them (Bug #56703).

2.4 Univention App Center

- A broken internal JSON file will no longer crash the **univention-appcenter-listener-converter**. If a broken JSON file is found, it will be skipped and logged in the log file `/var/log/univention/listener_modules/<app id>.log` (Bug #56421).

2.5 Univention Directory Manager and command line interface

- The `If-Match` request header can now be given in `DELETE` requests to the UDM REST API to make them conditional (Bug #56731).
- Missing properties when creating or modifying objects via the UDM REST API are now correctly marked in the error response (Bug #56734).
- The unused UDM properties from Nagios server have been marked as optional to ease the upgrade to UCS 5.2 (Bug #56820).
- The Python 3.11 compatibility for timezone handling has been repaired (Bug #56514).
- The case sensitivity of the attribute `memberUid` is now respected when removing members from a group (Bug #54183).
- The command **univention-admin** has been removed. It was deprecated since UCS 3.0 (Bug #53802).

2.6 Modules for system settings / setup wizard

- The process to renew all SSL/TLS certificates has been improved. For each host the symbolic link pointing to the fully-qualified host name is now created as a relative link. Error cases are better detected and handled. All changed SSL/TLS profile settings are now propagated into a new CA certificate. The policy enforced by OpenSSL on the certificate settings is now also checked and enforced in the UMC module *Certificate settings* (Bug #34106).
- The connection check to the package repository now explicitly uses the proxy settings (Bug #48126).

2.7 Domain join module

- The join-scripts are now executed with `umask 022` instead of the restrictive `umask 077` from the UMC Server (Bug #53431).

2.8 System diagnostic module

- Include new diagnostic module to check if PostgreSQL is migrated to version 11 (Bug #56773).
- The text *Success* is no longer displayed when a check failed after all checks have previously passed (Bug #56624).
- Include new diagnostic module to check the correct setting of Univention Configuration Registry Variable `ldap/master` (Bug #48548).

2.9 File system quota module

- Querying users for a partition runs into a timeout after 10 minutes when there are many users (Bug #56575).

CHAPTER

THREE

UNIVENTION BASE LIBRARIES

- The registration of LDAP schema files failed if the schema file is the first file in the directory and there is already a local schema file with the same name which was not registered via LDAP (Bug #56857).
- The unused LDAP attributes from Nagios server have been marked as optional to ease the upgrade to UCS 5.2 (Bug #56820).
- UCS 5.0 erratum 785 introduced a new mechanism in **ucs_registerLDAPExtension** to re- trigger the activation of an LDAP ACL or schema extension by doing a trivial (i.e. no-op) LDAP modification. This failed on the Primary node due to missing credentials. **ucs_registerLDAPExtension** has been fixed to use the LDAP admin connection in this case (Bug #56698).
- The program **univention-backup2master** has been improved and handles more corner-cases correctly. Entries of other hosts are now skipped, whose name only contains the name of the old Primary as a sub-string. Handling of shares, mail, host, and service records has been reworked (Bug #46062).

CHAPTER

FOUR

SOFTWARE DEPLOYMENT

- The software update module will not show *UCS 5.1-0* as available version for upgrade because it is an intermediate version between UCS 5.0 and UCS 5.2 to which an upgrade will not be possible (Bug #56517).
- The internal tool **`ucslint`** is now independent from the current working directory. It has been fully converted to Python 3.7 code, which changes the API for its plugins. Performance has also been improved and several small bugs have been fixed. This found several new issues in other packages, which previously had not been detected. Some of them have also been fixed (Bug #55668).

CHAPTER

FIVE

SYSTEM SERVICES

5.1 SAML

- **univention-keycloak init** is now able to be executed again in case of a failure during first initialization. The option `--force` has been added to force the rerun of the initialization (Bug #56791).
- A script which checks the migration status from SimpleSAMLPHP / OpenID Connector Provider to Keycloak has been added to the package **univention-keycloak** (Bug #56747).
- The commands **messages** and **login-links** have been added to manage Keycloak message bundles and login links for the login page (Bug #56478).
- The Python 2.7 compatibility for the Univention Configuration Registry template file `/etc/simplesamlphp/00authsources.php` has been restored (Bug #56588) and was ported back to UCS 5.0-4 (Bug #56647).
- A workaround has been added which prevents a potential LDAP schema registration failure (Bug #56857).
- UCS 5.0 erratum 881 broke mixed environments with UCS 4.4. Therefore the UDM modules are now only registered for UCS 5 based systems (Bug #56864).
- The LDAP schema and UDM modules are now registered in the LDAP and therefore replicated to all servers in the domain to ease the upgrade to UCS 5.2 (Bug #56824).

5.2 Mail services

- The detection whether a user is a **Fetchmail** user (by checking if they have an attribute `mailPrimaryAddress`) during modifications of users has been repaired. Therefore when the `mailPrimaryAddress` is changed or removed the correct changes are synchronized to **Fetchmail** (Bug #56482).
- Deleting **Fetchmail** configurations of a user now correctly removes entries from the file `fetchmailrc` in case they are the last ones (Bug #56426).
- Narrowed down the conditions under which the Univention Directory Listener module gets called (Bug #56586).

5.3 SSL

- The missing dependency on the package **ca-certificate** has been added as the common root Certificate Authority certificates are required to access public services like the Univention download server (Bug #51203).
- Certificate identifiers are now compared as strings. Previously certain identifiers like `2e2` had been handles as floating-point numbers in scientific notations by **awk** (Bug #54834).

5.4 DHCP server

- The network installer has been converted from a SysV init script into a **systemd** unit. URLs configured for Univention Configuration Registry Variable `repository/online/server` are now handled correctly.

5.5 PAM / Local group cache

- Future compatibility with **sudo** version 1.9.4 has been added, where additional environment variables need to be passed explicitly to sub-processes (Bug #56579).

CHAPTER

SIX

SERVICES FOR WINDOWS

6.1 Samba

- **univention-samba4-backup** now uses the **samba-tool** backup command to create a backup of the Samba database and the directory `syslog` (Bug #56434).
- The Univention Configuration Registry Variables `samba/database/backend/store` and `samba/database/backend/store/size` have been added to configure the Samba database backend (`tdb` or `mdb`) before the initial setup, join or re-join (Bug #56401).
- The Samba package now recommends the package **python3-lmdb** (Bug #53387).
- Under certain conditions, installation of the package **univention-samba4** aborted because of a missing package dependency on a specific version of **samba-dsdb-modules**, when an older version of that package was already installed. This is addressed by making the package **univention-samba4** depend on the meta-package **samba-ad-dc** instead, and letting that manage a versioned dependency on **samba-dsdb-modules**. This simplifies the package dependencies (Bug #56794).
- The package **samba-ad-dc** now depends on a specific version of **samba-dsdb-modules** to upgrade the initially installed version to the one required during installation. This addresses issues when an ISO was used for installation that did not already include the latest Samba provided by errata updates (Bug #56794).
- The package **samba-ad-dc** now depends on a specific version of **samba-ad-provision**, instead of only recommending it. This addresses issues when installing directly from the UCS 5.0-6 ISO image (Bug #56870).
- The modified dependency of **univention-samba4** on **samba-ad-dc** introduced by UCS 5.0 erratum 890 caused **libnss-winbind** to be installed. This package modified file:*/etc/nsswitch.conf* adding `winbind` to it. This has been reverted (Bug #56885).
- Symbolic links in the directory `sysvol` will no longer break the Samba backup tool (Bug #56866).

6.2 Univention S4 Connector

- Starting with UCS 5.0 the Univention S4 connector converted POSIX-only groups to Samba groups. This was a regression compared to the behavior in UCS 4.4. Now the mapping offers a new key `auto_enable_udm_option` that is disabled by default and is only activated for the UDM property `userCertificate`, allowing changes of UDM object options just in that special case (Bug #56772).
- Future compatibility for **python3-ldap** >= 4 has been added (Bug #56603).
- Future compatibility for **python3-samba** has been added (Bug #56537).

6.3 Univention Active Directory Connection

- During synchronization from an MS AD forest child domain, the Univention AD connector may receive DNs that refer to objects outside the scope of the child domain. In that case it receives an LDAP referral which caused a python traceback. The Univention AD connector now skips referrals to objects and logs an informative message instead (Bug #56792).
- The Univention AD connector failed to handle forest child domains (Bug #53944).
- Future compatibility for **`python3-ldap`** >= 4 has been added (Bug #56603).

INDEX

B

Bugzilla
    Bug #34106, 6
    Bug #46062, 9
    Bug #48126, 6
    Bug #48548, 6
    Bug #51203, 14
    Bug #53387, 3, 15
    Bug #53431, 6
    Bug #53802, 6
    Bug #53860, 5
    Bug #53944, 16
    Bug #54183, 6
    Bug #54834, 14
    Bug #55668, 11
    Bug #56005, 3
    Bug #56046, 3
    Bug #56198, 5
    Bug #56332, 2
    Bug #56333, 2
    Bug #56349, 5
    Bug #56354, 2
    Bug #56401, 15
    Bug #56421, 6
    Bug #56426, 13
    Bug #56434, 15
    Bug #56478, 13
    Bug #56482, 13
    Bug #56510, 5
    Bug #56514, 6
    Bug #56517, 11
    Bug #56537, 15
    Bug #56548, 5
    Bug #56562, 5
    Bug #56575, 5, 7
    Bug #56579, 14
    Bug #56586, 13
    Bug #56588, 13
    Bug #56603, 15, 16
    Bug #56607, 1
    Bug #56608, 1
    Bug #56624, 6
    Bug #56632, 2
    Bug #56633, 2
    Bug #56644, 2
    Bug #56647, 13
    Bug #56652, 1
    Bug #56653, 2
    Bug #56654, 2
    Bug #56655, 2
    Bug #56660, 5
    Bug #56675, 3
    Bug #56676, 1
    Bug #56677, 2
    Bug #56678, 2
    Bug #56679, 1
    Bug #56683, 2
    Bug #56684, 2
    Bug #56696, 2
    Bug #56698, 9
    Bug #56703, 5
    Bug #56706, 1
    Bug #56714, 5
    Bug #56729, 3
    Bug #56731, 5, 6
    Bug #56734, 5, 6
    Bug #56738, 2
    Bug #56739, 2
    Bug #56740, 2
    Bug #56741, 2
    Bug #56742, 2
    Bug #56743, 2
    Bug #56744, 2
    Bug #56745, 1
    Bug #56746, 2
    Bug #56747, 13
    Bug #56753, 5
    Bug #56755, 2
    Bug #56767, 2
    Bug #56772, 15
    Bug #56773, 6
    Bug #56776, 2
    Bug #56777, 3
    Bug #56778, 1
    Bug #56779, 2
    Bug #56780, 1
    Bug #56791, 13
    Bug #56792, 16
    Bug #56794, 15
    Bug #56801, 3
    Bug #56820, 6, 9
    Bug #56821, 2

Bug #56822, 2
Bug #56824, 13
Bug #56828, 5
Bug #56857, 9, 13
Bug #56864, 13
Bug #56866, 15
Bug #56870, 15
Bug #56876, 1
Bug #56877, 2
Bug #56885, 15
Bug #56892, 2
Bug #56893, 2

C

CVE

CVE-2018-20060, 2
CVE-2018-25091, 2
CVE-2019-11236, 2
CVE-2019-11324, 2
CVE-2019-19450, 2
CVE-2020-11080, 2
CVE-2020-19189, 2
CVE-2020-21047, 1
CVE-2020-21710, 2
CVE-2020-21890, 2
CVE-2020-22217, 1
CVE-2020-22219, 2
CVE-2020-23804, 2
CVE-2020-25648, 2
CVE-2020-26137, 2
CVE-2020-28463, 2
CVE-2021-23336, 2
CVE-2021-39537, 2
CVE-2022-0391, 2
CVE-2022-2505, 1
CVE-2022-23597, 1
CVE-2022-27635, 2
CVE-2022-36315, 1
CVE-2022-36316, 1
CVE-2022-36318, 1
CVE-2022-36319, 1
CVE-2022-36320, 1
CVE-2022-36351, 2
CVE-2022-37050, 2
CVE-2022-37051, 2
CVE-2022-38076, 2
CVE-2022-38472, 1
CVE-2022-38473, 1
CVE-2022-38475, 1
CVE-2022-38477, 1
CVE-2022-38478, 1
CVE-2022-40674, 1
CVE-2022-40956, 1
CVE-2022-40957, 1
CVE-2022-40958, 1
CVE-2022-40959, 1
CVE-2022-40960, 1
CVE-2022-40962, 1
CVE-2022-40964, 2
CVE-2022-42927, 1
CVE-2022-42928, 1
CVE-2022-42929, 1
CVE-2022-42930, 1
CVE-2022-42931, 1
CVE-2022-42932, 1
CVE-2022-45403, 1
CVE-2022-45404, 1
CVE-2022-45405, 1
CVE-2022-45406, 1
CVE-2022-45407, 1
CVE-2022-45408, 1
CVE-2022-45409, 1
CVE-2022-45410, 1
CVE-2022-45411, 1
CVE-2022-45412, 1
CVE-2022-45415, 1
CVE-2022-45416, 1
CVE-2022-45417, 1
CVE-2022-45418, 1
CVE-2022-45419, 1
CVE-2022-45420, 1
CVE-2022-45421, 1
CVE-2022-46329, 2
CVE-2022-46871, 1
CVE-2022-46872, 1
CVE-2022-46873, 1
CVE-2022-46874, 1
CVE-2022-46877, 1
CVE-2022-46878, 1
CVE-2022-46879, 1
CVE-2022-48560, 2
CVE-2022-48564, 2
CVE-2022-48565, 2
CVE-2022-48566, 2
CVE-2022-48571, 2
CVE-2023-0767, 1
CVE-2023-2454, 2
CVE-2023-2455, 2
CVE-2023-3482, 1
CVE-2023-3600, 1
CVE-2023-3961, 2
CVE-2023-4045, 1
CVE-2023-4046, 1
CVE-2023-4047, 1
CVE-2023-4048, 1
CVE-2023-4049, 1
CVE-2023-4050, 1
CVE-2023-4051, 1
CVE-2023-4053, 1
CVE-2023-4055, 1
CVE-2023-4056, 1
CVE-2023-4057, 1
CVE-2023-4091, 2
CVE-2023-4154, 2
CVE-2023-4421, 2
CVE-2023-4504, 1

CVE-2023-4573, 1
CVE-2023-4574, 1
CVE-2023-4575, 1
CVE-2023-4577, 1
CVE-2023-4578, 1
CVE-2023-4580, 1
CVE-2023-4581, 1
CVE-2023-4583, 1
CVE-2023-4584, 1
CVE-2023-4585, 1
CVE-2023-4692, 2
CVE-2023-4693, 2
CVE-2023-4752, 3
CVE-2023-4781, 3
CVE-2023-4863, 1, 2
CVE-2023-5169, 1
CVE-2023-5171, 1
CVE-2023-5176, 1
CVE-2023-5217, 1
CVE-2023-5367, 3
CVE-2023-5380, 3
CVE-2023-5721, 1
CVE-2023-5724, 1
CVE-2023-5725, 1
CVE-2023-5728, 1
CVE-2023-5730, 1
CVE-2023-5732, 1
CVE-2023-5868, 2
CVE-2023-5869, 2
CVE-2023-5870, 2
CVE-2023-5981, 2
CVE-2023-6204, 1
CVE-2023-6205, 1
CVE-2023-6206, 1
CVE-2023-6207, 1
CVE-2023-6208, 1
CVE-2023-6209, 1
CVE-2023-6212, 1
CVE-2023-21930, 2
CVE-2023-21937, 2
CVE-2023-21938, 2
CVE-2023-21939, 2
CVE-2023-21954, 2
CVE-2023-21967, 2
CVE-2023-21968, 2
CVE-2023-22006, 2
CVE-2023-22036, 2
CVE-2023-22041, 2
CVE-2023-22045, 2
CVE-2023-22049, 2
CVE-2023-22081, 2
CVE-2023-23598, 1
CVE-2023-23601, 1
CVE-2023-23602, 1
CVE-2023-23603, 1
CVE-2023-23604, 1
CVE-2023-23605, 1
CVE-2023-23606, 1
CVE-2023-24329, 2
CVE-2023-25193, 2
CVE-2023-25728, 1
CVE-2023-25729, 1
CVE-2023-25730, 1
CVE-2023-25731, 1
CVE-2023-25732, 1
CVE-2023-25733, 1
CVE-2023-25735, 1
CVE-2023-25736, 1
CVE-2023-25737, 1
CVE-2023-25739, 1
CVE-2023-25741, 1
CVE-2023-25742, 1
CVE-2023-25744, 1
CVE-2023-25745, 1
CVE-2023-25750, 1
CVE-2023-25751, 1
CVE-2023-25752, 1
CVE-2023-27102, 2
CVE-2023-27103, 2
CVE-2023-28160, 1
CVE-2023-28161, 1
CVE-2023-28162, 1
CVE-2023-28164, 1
CVE-2023-28176, 1
CVE-2023-28177, 1
CVE-2023-28321, 1
CVE-2023-29491, 2
CVE-2023-29499, 2
CVE-2023-29533, 1
CVE-2023-29535, 1
CVE-2023-29536, 1
CVE-2023-29537, 1
CVE-2023-29538, 1
CVE-2023-29539, 1
CVE-2023-29540, 1
CVE-2023-29541, 1
CVE-2023-29543, 1
CVE-2023-29544, 1
CVE-2023-29547, 1
CVE-2023-29548, 1
CVE-2023-29549, 1
CVE-2023-29550, 1
CVE-2023-29551, 1
CVE-2023-32205, 1
CVE-2023-32206, 1
CVE-2023-32207, 1
CVE-2023-32208, 1
CVE-2023-32209, 1
CVE-2023-32210, 1
CVE-2023-32211, 1
CVE-2023-32212, 1
CVE-2023-32213, 1
CVE-2023-32215, 1
CVE-2023-32216, 1
CVE-2023-32360, 1
CVE-2023-32611, 2

CVE-2023-32665, 2
CVE-2023-34414, 1
CVE-2023-34415, 1
CVE-2023-34416, 1
CVE-2023-34417, 1
CVE-2023-34969, 1
CVE-2023-36054, 2
CVE-2023-37201, 1
CVE-2023-37202, 1
CVE-2023-37203, 1
CVE-2023-37204, 1
CVE-2023-37205, 1
CVE-2023-37206, 1
CVE-2023-37207, 1
CVE-2023-37208, 1
CVE-2023-37209, 1
CVE-2023-37210, 1
CVE-2023-37211, 1
CVE-2023-37212, 1
CVE-2023-38546, 1
CVE-2023-38994, 2
CVE-2023-40217, 2
CVE-2023-42114, 1
CVE-2023-42116, 1
CVE-2023-42669, 2
CVE-2023-42670, 2
CVE-2023-43785, 2
CVE-2023-43786, 2
CVE-2023-43787, 2
CVE-2023-43788, 2
CVE-2023-43789, 2
CVE-2023-43803, 2
CVE-2023-43804, 2
CVE-2023-43887, 2
CVE-2023-44487, 2
CVE-2023-47471, 2

D

directory/manager/rest/html-view-enabled, 5

E

environment variable
directory/manager/rest/html-view-enabled, 5
ldap/master, 6
repository/online/server, 14
samba/database/backend/store, 15
samba/database/backend/store/size, 15
Errata updates
UCS 5.0 erratum 721, 5
UCS 5.0 erratum 785, 9
UCS 5.0 erratum 870, 3
UCS 5.0 erratum 881, 13
UCS 5.0 erratum 890, 15

L

ldap/master, 6

R

repository/online/server, 14

S

samba/database/backend/store, 15
samba/database/backend/store/size, 15