



# **Changelog for Univention Corporate Server (UCS) 5.0-5**

*Release 5.0-5*

**Nov 15, 2023**

The source of this document is licensed under GNU Affero General Public License v3.0 only.

# CONTENTS

<b>1</b>	<b>General</b>	<b>1</b>
1.1	OpenLDAP . . . . .	2
<b>2</b>	<b>Univention Management Console</b>	<b>3</b>
2.1	Univention Management Console web interface . . . . .	3
2.2	Univention Portal . . . . .	3
2.3	Univention Management Console server . . . . .	3
2.4	Univention App Center . . . . .	4
2.5	Univention Directory Manager and command line interface . . . . .	4
2.6	Modules for system settings / setup wizard . . . . .	5
2.7	Domain join module . . . . .	5
2.8	System diagnostic module . . . . .	5
2.9	Univention Configuration Registry module . . . . .	5
2.10	Other modules . . . . .	5
2.11	Development of modules for Univention Management Console . . . . .	6
<b>3</b>	<b>Univention base libraries</b>	<b>7</b>
<b>4</b>	<b>System services</b>	<b>9</b>
4.1	SAML . . . . .	9
4.2	Univention self service . . . . .	9
4.3	Mail services . . . . .	9
4.4	Spam/virus detection and countermeasures . . . . .	10
4.5	Nagios . . . . .	10
4.6	RADIUS . . . . .	10
4.7	PAM / Local group cache . . . . .	10
<b>5</b>	<b>Services for Windows</b>	<b>11</b>
5.1	Samba . . . . .	11
5.2	Univention S4 Connector . . . . .	11
5.3	Univention Active Directory Connection . . . . .	12
	<b>Index</b>	<b>13</b>



## GENERAL

- All security updates issued for UCS 5.0-4 are included:
  - **amd64-microcode** (CVE-2019-9836, CVE-2023-20593) (Bug #56386)
  - **avahi** (CVE-2021-3468) (Bug #56199)
  - **bind9** (CVE-2023-2828) (Bug #56345)
  - **c-ares** (CVE-2023-31130, CVE-2023-32067) (Bug #56236)
  - **clamav** (CVE-2023-20197) (Bug #56496)
  - **cups** (CVE-2023-34241) (Bug #56244)
  - **firefox-esr** (CVE-2023-37201, CVE-2023-37202, CVE-2023-37207, CVE-2023-37208, CVE-2023-37211, CVE-2023-4045, CVE-2023-4046, CVE-2023-4047, CVE-2023-4048, CVE-2023-4049, CVE-2023-4050, CVE-2023-4055, CVE-2023-4056, CVE-2023-4573, CVE-2023-4574, CVE-2023-4575, CVE-2023-4581, CVE-2023-4584) (Bug #56299, Bug #56432, Bug #56513)
  - **ghostscript** (CVE-2023-38559) (Bug #56414)
  - **intel-microcode** (CVE-2022-40982, CVE-2022-41804, CVE-2023-23908) (Bug #56462)
  - **libfastjson** (CVE-2020-12762) (Bug #56179)
  - **libssh2** (CVE-2019-13115, CVE-2019-17498, CVE-2020-22218) (Bug #56563)
  - **libx11** (CVE-2023-3138) (Bug #56245)
  - **libxpm** (CVE-2022-44617, CVE-2022-46285, CVE-2022-4883) (Bug #56178)
  - **linux** (CVE-2022-40982, CVE-2023-1380, CVE-2023-2002, CVE-2023-2007, CVE-2023-20593, CVE-2023-2269, CVE-2023-3090, CVE-2023-31084, CVE-2023-3111, CVE-2023-3141, CVE-2023-32233, CVE-2023-3268, CVE-2023-3338, CVE-2023-34256, CVE-2023-35788, CVE-2023-35823, CVE-2023-35824) (Bug #56376, Bug #56430)
  - **linux-latest** (CVE-2023-1380, CVE-2023-2002, CVE-2023-2007, CVE-2023-20593, CVE-2023-2269, CVE-2023-3090, CVE-2023-31084, CVE-2023-3111, CVE-2023-3141, CVE-2023-32233, CVE-2023-3268, CVE-2023-3338, CVE-2023-34256, CVE-2023-35788, CVE-2023-35823, CVE-2023-35824) (Bug #56376)
  - **linux-signed-amd64** (CVE-2022-40982, CVE-2023-1380, CVE-2023-2002, CVE-2023-2007, CVE-2023-20593, CVE-2023-2269, CVE-2023-3090, CVE-2023-31084, CVE-2023-3111, CVE-2023-3141, CVE-2023-32233, CVE-2023-3268, CVE-2023-3338, CVE-2023-34256, CVE-2023-35788, CVE-2023-35823, CVE-2023-35824) (Bug #56376, Bug #56430)
  - **lua5.3** (CVE-2019-6706, CVE-2020-24370) (Bug #56200)
  - **memcached** (CVE-2022-48571) (Bug #56560)
  - **openssh** (CVE-2023-38408) (Bug #56463)
  - **php7.3** (CVE-2023-3247, CVE-CVE-2023-3823, CVE-CVE-2023-3824) (Bug #56180, Bug #56549)

- **poppler** (CVE-2020-36023, CVE-2020-36024) (Bug #56431)
  - **python3.7** (CVE-2015-20107, CVE-2020-10735, CVE-2021-3426, CVE-2021-3733, CVE-2021-3737, CVE-2021-4189, CVE-2022-45061) (Bug #56243)
  - **samba** (CVE-2022-2127, CVE-2023-3347, CVE-2023-34966, CVE-2023-34967, CVE-2023-34968) (Bug #56297, Bug #56320)
  - **systemd** (CVE-2022-3821) (Bug #56237)
  - **tiff** (CVE-2023-25433, CVE-2023-26965, CVE-2023-26966, CVE-2023-2908, CVE-2023-3316, CVE-2023-3618, CVE-2023-38288, CVE-2023-38289) (Bug #56388)
  - **qpdf** (CVE-2018-18020, CVE-2021-25786, CVE-2021-36978) (Bug #56507)
  - **yajl** (CVE-2017-16516, CVE-2022-24795, CVE-2023-33460) (Bug #56242, Bug #56325)
- The following updated packages from Debian 10.13 are included: **aom bouncycastle burp cjose datatables.js debian-archive-keyring docker-registry elixir-lang erlang flask flask-security fusiondirectory golang-yaml.v2 gst-plugins-bad1.0 gst-plugins-base1.0 gst-plugins-good1.0 gst-plugins-ugly1.0 hdf5 hsqldb hsqldb1.8.0 iperf3 lemonldap-ng libapache2-mod-auth-openidc libhtml-cleaner-java libmail-dkim-perl libraw libreoffice libusrctp linux-5.10 linux-signed-5.10-amd64 lxc mediawiki minidlna netatalk node-tough-cookie nsis ocsinventory-server opendmarc openimageio opensc openssl open-vm-tools otrs2 owslib pandoc pdfcrack php-cas php-dompdf pypdf2 python-django python-git python-mechanize qt4-x11 rabbitmq-server rar renderdoc ring ruby-doorkeeper ruby-redcloth sox symfony thunderbird trafficserver tryton-server unrar-nonfree w3m wordpress xmltooling zabbix**

## 1.1 OpenLDAP

### 1.1.1 Listener/Notifier domain replication

- The rotation for the Univention Directory Listener module log file is now done by **logrotate** and it can be configured via Univention Configuration Registry (Bug #55610).

## UNIVENTION MANAGEMENT CONSOLE

### 2.1 Univention Management Console web interface

- When computer objects were assigned with a network the DHCP and DNS settings weren't saved if a custom IP was specified (Bug #55459).
- Accessing objects which contain UTF-8 characters in their LDAP DN was impossible and has been fixed (Bug #56189).
- The displayed description of objects is now more accurate, for example for OX IMAP folder objects did not include the domain name which made it difficult to differentiate folder names for different domains (Bug #50632).
- A username enumeration vulnerability in the UDM REST API has been corrected (Bug #56351).
- Creating multiple objects from the same template resulted in overwritten shared references to link-relations in the UDM REST API Python Client leading to wrong `object exists` error messages (Bug #56271).
- New CSS variables have been introduced in the standard themes `dark` and `light`. These will be needed for the Keycloak login page. Custom themes will have sane defaults (Bug #56458).
- The text color for disabled text boxes has been changed so it is easier to read in the Safari browser (Bug #55939).
- The login will show the cookie banner only if it is configured via the new Univention Configuration Registry Variable `umc/cookie-banner/domains` (Bug #55164).

### 2.2 Univention Portal

- The navigation endpoint now correctly detects access via HTTPS and returns URLs based on that if no base URL is passed (Bug #55785).
- The portal will show the cookie banner only if it is configured via the new Univention Configuration Registry Variable `umc/cookie-banner/domains` (Bug #55164).

### 2.3 Univention Management Console server

- Connection timeouts during requests to UMC modules are now handled in the UMC server so that timed out requests don't prevent a session timeout (Bug #56198).
- In multiprocessing mode of the UMC-Server the SAML login could cause corrupted BDB SAML Identity Cache databases (Bug #56303).
- Aborted HTTP requests do not close the socket connection to still opened UMC module processes anymore but wait until the session times out (Bug #56336).
- New Python APIs for modules are provided which help in replacing `python-notifier` (Bug #56201).

- The link to the Univention Wiki has been removed because it's deprecated and planned for going offline (Bug #56357).
- The UMC ACL's are now loaded from the local LDAP server again. This was broken since UCS 5.0-4 (Bug #56330).
- The Self-Service was broken on DC Backups since UCS 5.0-4 because incoming requests that were forwarded to the DC Primary contained broken request paths that led to 403 Forbidden error messages saying "No module found for this request." (Bug #56335).
- Aborted HTTP requests no longer prevent the module from properly shutting down (Bug #56391).
- The translation of messages from UMC module processes has been repaired in certain scenarios (Bug #56256).
- The UMC module has been adjusted to use new Python APIs for modules (Bug #56201).
- The new Univention Configuration Registry Variable `umc/cookie-banner/domains` can be used to configure on which domains to show the cookie banner. Additionally, top level domains can be configured so that the cookie can be shared between portal and login page. By default, both portal and login page will always show the cookie banner and not share it (Bug #55164).

## 2.4 Univention App Center

- A typo in the output of `univention-app stall --help` has been fixed (Bug #56047).
- The UMC module has been adjusted to use new Python APIs for modules (Bug #56201).

## 2.5 Univention Directory Manager and command line interface

- The performance of move operations for users and computers has been improved, which is especially significant when the moved object is a member of a large group (Bug #56348).
- The URI when creating a printer with the UDM CLI now doesn't require a space between protocol and path anymore (Bug #24081).
- The German word *Kennwort* has been replaced with *Passwort* to make the German translation of UCS more consistent (Bug #56371).
- Nested lists (e.g. links of portal entries) are now parsed correctly by the UDM REST API server (Bug #56271).
- Under certain circumstances the module `users/user` could skip updating the attribute `univention-LastUsedValue` at the object `cn=uidNumber` in LDAP (Bug #56309).
- When computer objects were assigned with a network the DHCP and DNS settings weren't saved if a custom IP was specified (Bug #55459).
- Values for the syntax class `complex` can now contain double quotes (Bug #27241).
- It is possible again to detect, search and modify objects `users/ldap` which have `univentionObject-Flag=functional` (Bug #55216).
- The displayed description of objects is now more accurate, for example for OX IMAP folder objects did not include the domain name which made it difficult to differentiate folder names for different domains (Bug #50632).
- The class `AttributeHook` was not idempotent and caused errors when multiple `open()` calls have been done. This is for example the case in the `UCS@school` importer (Bug #56036).



## 2.6 Modules for system settings / setup wizard

- The UMC module has been adjusted to use new Python APIs for modules (Bug #56201).
- The link to the Univention Wiki has been removed from the privacy statement in the system setup. Univention Wiki is deprecated and planned for going offline (Bug #56357).

## 2.7 Domain join module

- The UMC module has been adjusted to use new Python APIs for modules (Bug #56201).
- The default timeout for initial replication of the DNS host record of a joining system can now be adjusted by making use of the new Univention Configuration Registry Variable `join/samba/dns/replication/timeout` which has the old default value of 600 seconds. This is only necessary in large environments where the initial replication from UDM/OpenLDAP to Samba/AD may be delayed due to a large number of objects (Bug #55937).
- The script `univention-check-join-status` called `ldapsearch` with the machine credentials, which then were visible in the process list (Bug #56331).

## 2.8 System diagnostic module

- Read-only loop devices and `squashfs` file systems are now ignored by the disk usage check (Bug #56109).

## 2.9 Univention Configuration Registry module

- If a Univention Configuration Registry Variable is changed to an empty value via UMC, a confirmation dialog is displayed to let the user decide on whether to store an empty string or to actually delete the variable (Bug #55517).

## 2.10 Other modules

- If the name of an LDAP object consists only of numbers and these start with zeros, these zeros are no longer removed (Bug #56338).
- The UMC module has been adjusted to use new Python APIs for modules (Bug #56201).
- When computer objects were assigned with a network the DHCP and DNS settings weren't saved if a custom IP was specified. This has been corrected (Bug #55459).
- The displayed description of objects is now more accurate, for example for OX IMAP folder objects did not include the domain name which made it difficult to differentiate folder names for different domains (Bug #50632).

## 2.11 Development of modules for Univention Management Console

- The UMC module has been adjusted to use new Python APIs for modules (Bug #56201).

## UNIVENTION BASE LIBRARIES

- In case an LDAP ACL or schema extension got installed by a joinscript by running the function `ucs_registerLDAPExtension` and it was not activated for some reason (e.g. because the **slapd** was not running at the time when the postrun of the `ldap_extension` listener module was running) a rerun of **univention-run-join-scripts** did not change anything. Now `ucs_registerLDAPExtension` has been adjusted to do a trivial (i.e. no-op) LDAP modification to re-trigger activation ([Bug #55337](#)).
- A regression in [UCS 5.0 erratum 683](#) has been corrected, which caused the Debian package manager APT to print many errors while reporting progress to UMC ([Bug #56162](#)).



## SYSTEM SERVICES

### 4.1 SAML

- The creation of the SAML Identity Provider user accounts during the installation ignores the password length and history (Bug #49207).
- The German word *Kennwort* has been replaced with *Passwort* to make the German translation of UCS more consistent (Bug #56371).
- The new Univention Configuration Registry Variable `ucs/server/sso/password/change/server` allows to configure the server used for password changes during the SSO login. The default (the local server) is not changed with this update (Bug #55203).
- It is now possible to set option Keycloak clients authentication flow using `client-auth-flow`. Passing an empty string will reset the flow to the default browser flow (Bug #56317).
- The command `legacy-authentication-flow` has been added to create an authentication flow which will enable app specific authorization in a future version of the Keycloak App (Bug #56305).
- The setting `ldapsOnly` for the option `useTruststoreSpi` in the LDAP federation configuration has been removed. We now set `never` during the update and for new installations (Bug #56484).
- The command `get-keycloak-base-url` has been added to `univention-keycloak` to get the current base URL for the Keycloak server (Bug #56132).
- Added parameters for creating SAML service providers to `univention-keycloak` (Bug #56132).
- The tool `univention-keycloak` has been updated to configure Kerberos ticket authentication in Keycloak (Bug #56153).

### 4.2 Univention self service

- The UMC module has been adjusted to use new Python APIs for modules (Bug #56201).

### 4.3 Mail services

- The values of `univentionFetchmailSingle` and `univentionFetchmailMulti` can't be correctly parsed when the values contain characters like `;`. The property is now stored as JSON to simplify the parsing of the complex attribute and avoid errors when non-alphanumeric characters appear. The fix is applied after force-re-executing the `joinscript 92univention-fetchmail-schema.inst`. If `fetchmail` is installed on a non-primary server, the primary and non-primary servers need to be updated to the same errata level before force-re-executing the `joinscript` to minimize possible unknown side effects (Bug #56008).
- The Fetchmail UDM hooks did not work in combination with the `UCS@school` importer. They are now compatible after force-re-executing the `joinscript 92univention-fetchmail-schema.inst` (Bug #56036).

- Increased `univention-fetchmail-schema` joinscript version to automatically apply fix for [Bug #56008](#). Added logic to correctly handle bytes in `migrate-fetchmail.py` script and `fetchmail.py` hook ([Bug #56308](#)).

### 4.4 Spam/virus detection and countermeasures

- The type of the Univention Configuration Registry Variable `mail/antispam/requiredhits` only allowed to set integer values while the SpamAssassin configuration also allows real numbers. The type definition has therefore been adjusted to allow all possible values ([Bug #55685](#)).

### 4.5 Nagios

- The check `check_univention_joinstatus` called `ldapsearch` with the machine credentials, which then were visible in the process list ([Bug #56324](#)).
- The metrics are now written using the official `python3-prometheus-client` library and contain timestamps so they can be evaluated more accurately ([Bug #55367](#)).
- [UCS 5.0 erratum 743](#) introduced an incompatibility with `prometheus-node-exporter` which disallows timestamps to be present in the text-collector files. The change has therefore been reverted ([Bug #56341](#)).
- A metric in `check_univention_ad_connector` was missing the corresponding `connector` label and metrics were written for an invalid connector ([Bug #56350](#)).

### 4.6 RADIUS

- The German word *Kennwort* has been replaced with *Passwort* to make the German translation of UCS more consistent ([Bug #56371](#)).

### 4.7 PAM / Local group cache

- Samba/AD DC in UCS by default is configured with the parameter `obey pam restrictions = yes`, to allow the PAM session and account phases to operate on share access. This is used for example for automatic home directory creation. The corresponding PAM stack `samba` simply includes the generic `common-account` and `common-session` files, which make use of `pam_krb5` by default. This led to a situation where `pam_krb5` is run as part of the normal Samba login. Since that PAM module is linked to the Debian Heimdal base libraries which are using `pthreads` but Samba is using Heimdal libraries without `pthreads` over time this could lead to an resource depletion issue internal to `pthreads` and finally causing an `smbd` panic. To avoid this, we now adjusted the `common-account` and `common-session` files to skip `pam_krb5` for the service `samba`. At the point where these PAM modules are run in the context of Samba/AD, the authentication and Kerberos handling has already been done, so there is no point using `pam_krb5` functions in this case anyway ([Bug #56383](#)).

## SERVICES FOR WINDOWS

### 5.1 Samba

- The services `smbd` and `winbind` were not properly masked any longer on Samba/AD DCs. The need to be, because in that scenario, they are run as children of the main samba service (Bug #56187).
- The SPN account creation now ignores the password length and history (Bug #49207).
- The default timeout for initial replication of the DNS host record of a joining system can now be adjusted by making use of the new Univention Configuration Registry Variable `join/samba/dns/replication/timeout` which has the old default value of 600 seconds. This is only necessary in large environments where the initial replication from UDM/OpenLDAP to Samba/AD may be delayed due to a large number of objects (Bug #55937).
- The `samba` PAM stack included `common-auth` which is unnecessary in the context Samba/AD, because Samba/AD only uses the `account` and `session` phases of PAM (Bug #56383).
- The permissions of `/var/univention-backup/samba` were not restricted to user `root` and Domain Admins. By default in UCS ssh access to domain controllers is restricted to members of group “Domain Admins”, but this erratum implements tightened access control to that backup folder and the files created there (Bug #56499).

### 5.2 Univention S4 Connector

- To allow for a faster initial synchronization the connector now prioritizes objects of type `container/ou` (Bug #55938).
- By default `resync_object_from_ucs.py` now uses the local LDAP server for LDAP lookup. Use the option `--from-primary` for the old behavior (LDAP lookup on primary directory node, Bug #55936).
- The default timeout for initial replication of the DNS host record of a joining system can now be adjusted by making use of the new Univention Configuration Registry Variable `join/samba/dns/replication/timeout` which has the old default value of 600 seconds. This is only necessary in large environments where the initial replication from UDM/OpenLDAP to Samba/AD may be delayed due to a large number of objects (Bug #55937).

## 5.3 Univention Active Directory Connection

- By default `resync_object_from_ucs.py` now uses the local LDAP server for LDAP lookup. Use the option `--from-primary` for the old behavior (LDAP lookup on primary directory node, [Bug #55936](#)).



## INDEX

### B

#### Bugzilla

Bug #24081, 4  
Bug #27241, 4  
Bug #49207, 9, 11  
Bug #50632, 35  
Bug #55164, 3, 4  
Bug #55203, 9  
Bug #55216, 4  
Bug #55337, 7  
Bug #55367, 10  
Bug #55459, 35  
Bug #55517, 5  
Bug #55610, 2  
Bug #55685, 10  
Bug #55785, 3  
Bug #55936, 11, 12  
Bug #55937, 5, 11  
Bug #55938, 11  
Bug #55939, 3  
Bug #56008, 9, 10  
Bug #56036, 4, 9  
Bug #56047, 4  
Bug #56109, 5  
Bug #56132, 9  
Bug #56153, 9  
Bug #56162, 7  
Bug #56178, 1  
Bug #56179, 1  
Bug #56180, 1  
Bug #56187, 11  
Bug #56189, 3  
Bug #56198, 3  
Bug #56199, 1  
Bug #56200, 1  
Bug #56201, 36, 9  
Bug #56236, 1  
Bug #56237, 2  
Bug #56242, 2  
Bug #56243, 2  
Bug #56244, 1  
Bug #56245, 1  
Bug #56256, 4  
Bug #56271, 3, 4  
Bug #56297, 2  
Bug #56299, 1  
Bug #56303, 3  
Bug #56305, 9  
Bug #56308, 10  
Bug #56309, 4  
Bug #56317, 9  
Bug #56320, 2  
Bug #56324, 10  
Bug #56325, 2  
Bug #56330, 4  
Bug #56331, 5  
Bug #56335, 4  
Bug #56336, 3  
Bug #56338, 5  
Bug #56341, 10  
Bug #56345, 1  
Bug #56348, 4  
Bug #56350, 10  
Bug #56351, 3  
Bug #56357, 4, 5  
Bug #56371, 4, 9, 10  
Bug #56376, 1  
Bug #56383, 10, 11  
Bug #56386, 1  
Bug #56388, 2  
Bug #56391, 4  
Bug #56414, 1  
Bug #56430, 1  
Bug #56431, 2  
Bug #56432, 1  
Bug #56458, 3  
Bug #56462, 1  
Bug #56463, 1  
Bug #56484, 9  
Bug #56496, 1  
Bug #56499, 11  
Bug #56507, 2  
Bug #56513, 1  
Bug #56549, 1  
Bug #56560, 1  
Bug #56563, 1

### C

#### CVE

CVE-2015-20107, 2  
CVE-2017-16516, 2  
CVE-2018-18020, 2

CVE-2019-6706, 1  
CVE-2019-9836, 1  
CVE-2019-13115, 1  
CVE-2019-17498, 1  
CVE-2020-10735, 2  
CVE-2020-12762, 1  
CVE-2020-22218, 1  
CVE-2020-24370, 1  
CVE-2020-36023, 2  
CVE-2020-36024, 2  
CVE-2021-3426, 2  
CVE-2021-3468, 1  
CVE-2021-3733, 2  
CVE-2021-3737, 2  
CVE-2021-4189, 2  
CVE-2021-25786, 2  
CVE-2021-36978, 2  
CVE-2022-2127, 2  
CVE-2022-3821, 2  
CVE-2022-4883, 1  
CVE-2022-24795, 2  
CVE-2022-40982, 1  
CVE-2022-41804, 1  
CVE-2022-44617, 1  
CVE-2022-45061, 2  
CVE-2022-46285, 1  
CVE-2022-48571, 1  
CVE-2023-1380, 1  
CVE-2023-2002, 1  
CVE-2023-2007, 1  
CVE-2023-2269, 1  
CVE-2023-2828, 1  
CVE-2023-2908, 2  
CVE-2023-3090, 1  
CVE-2023-3111, 1  
CVE-2023-3138, 1  
CVE-2023-3141, 1  
CVE-2023-3247, 1  
CVE-2023-3268, 1  
CVE-2023-3316, 2  
CVE-2023-3338, 1  
CVE-2023-3347, 2  
CVE-2023-3618, 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-2023-4055, 1  
CVE-2023-4056, 1  
CVE-2023-4573, 1  
CVE-2023-4574, 1  
CVE-2023-4575, 1  
CVE-2023-4581, 1  
CVE-2023-4584, 1  
CVE-2023-20197, 1  
CVE-2023-20593, 1

CVE-2023-23908, 1  
CVE-2023-25433, 2  
CVE-2023-26965, 2  
CVE-2023-26966, 2  
CVE-2023-31084, 1  
CVE-2023-31130, 1  
CVE-2023-32067, 1  
CVE-2023-32233, 1  
CVE-2023-33460, 2  
CVE-2023-34241, 1  
CVE-2023-34256, 1  
CVE-2023-34966, 2  
CVE-2023-34967, 2  
CVE-2023-34968, 2  
CVE-2023-35788, 1  
CVE-2023-35823, 1  
CVE-2023-35824, 1  
CVE-2023-37201, 1  
CVE-2023-37202, 1  
CVE-2023-37207, 1  
CVE-2023-37208, 1  
CVE-2023-37211, 1  
CVE-2023-38288, 2  
CVE-2023-38289, 2  
CVE-2023-38408, 1  
CVE-2023-38559, 1  
CVE-CVE-2023-3823, 1  
CVE-CVE-2023-3824, 1

## E

environment variable  
  join/samba/dns/replication/time-  
    out, 5, 11  
  mail/antispam/requiredhits, 10  
  ucs/server/sso/pass-  
    word/change/server, 9  
  umc/cookie-banner/domains, 3, 4  
Errata updates  
  UCS 5.0 erratum 683, 7  
  UCS 5.0 erratum 743, 10

## J

join/samba/dns/replication/timeout, 5,  
11

## M

mail/antispam/requiredhits, 10

## U

ucs/server/sso/pass-  
  word/change/server, 9  
umc/cookie-banner/domains, 3, 4