univention
be open.

Changelog for Univention Corporate Server (UCS) 5.2-3

Release 5.2-3

Sep 08, 2025

CONTENTS

CHAPTER

ONE

GENERAL

- Univention Corporate Server 5.2-3 includes all security updates issued for UCS 5.2-2:
  - **firefox-esr** (CVE-2025-5263, CVE-2025-5264, CVE-2025-5266, CVE-2025-5267, CVE-2025-5268, CVE-2025-5269, CVE-2025-8027, CVE-2025-8028, CVE-2025-8029, CVE-2025-8030, CVE-2025-8031, CVE-2025-8032, CVE-2025-8033, CVE-2025-8034, CVE-2025-8035, CVE-2025-9179, CVE-2025-9180, CVE-2025-9181, CVE-2025-9185) (Bug #58441, Bug #58491, Bug #58540)
  - **gdk-pixbuf** (CVE-2025-6199) (Bug #58409)
  - **gnutls28** (CVE-2025-32988, CVE-2025-32989, CVE-2025-32990, CVE-2025-6395) (Bug #58480)
  - **icu** (CVE-2025-5222) (Bug #58439)
  - **jpeg-xl** (CVE-2023-0645, CVE-2023-35790, CVE-2024-11403, CVE-2024-11498) (Bug #58452)
  - **libxml2** (CVE-2022-49043, CVE-2023-39615, CVE-2023-45322, CVE-2024-25062, CVE-2024-34459, CVE-2024-56171, CVE-2025-24928, CVE-2025-27113, CVE-2025-32414, CVE-2025-32415) (Bug #58438)
  - **libxslt** (CVE-2023-40403, CVE-2024-55549, CVE-2025-24855, CVE-2025-7424) (Bug #58541)
  - **linux** (CVE-2024-26739, CVE-2024-26807, CVE-2024-28956, CVE-2024-35790, CVE-2024-36350, CVE-2024-36357, CVE-2024-36903, CVE-2024-36913, CVE-2024-36927, CVE-2024-38541, CVE-2024-41013, CVE-2024-43840, CVE-2024-53203, CVE-2024-53209, CVE-2024-56758, CVE-2024-57883, CVE-2025-21645, CVE-2025-21816, CVE-2025-21839, CVE-2025-21931, CVE-2025-22062, CVE-2025-22119, CVE-2025-23144, CVE-2025-27558, CVE-2025-37797, CVE-2025-37819, CVE-2025-37958, CVE-2025-37967, CVE-2025-38000, CVE-2025-38067, CVE-2025-38074, CVE-2025-38083, CVE-2025-38084, CVE-2025-38086, CVE-2025-38088, CVE-2025-38090, CVE-2025-38215, CVE-2025-38225, CVE-2025-38230) (Bug #58294, Bug #58528)
  - **linux-signed-amd64** (CVE-2024-26739, CVE-2024-26807, CVE-2024-28956, CVE-2024-35790, CVE-2024-36350, CVE-2024-36357, CVE-2024-36903, CVE-2024-36913, CVE-2024-36927, CVE-2024-38541, CVE-2024-41013, CVE-2024-43840, CVE-2024-53203, CVE-2024-53209, CVE-2024-56758, CVE-2024-57883, CVE-2025-21645, CVE-2025-21816, CVE-2025-21839, CVE-2025-21931, CVE-2025-22062, CVE-2025-22119, CVE-2025-23144, CVE-2025-27558, CVE-2025-37797, CVE-2025-37819, CVE-2025-37958, CVE-2025-37967, CVE-2025-38000, CVE-2025-38067, CVE-2025-38074, CVE-2025-38083, CVE-2025-38084, CVE-2025-38086, CVE-2025-38088, CVE-2025-38090, CVE-2025-38215, CVE-2025-38225, CVE-2025-38230) (Bug #58294, Bug #58528)
  - **openjdk-17** (CVE-2025-21587, CVE-2025-30691, CVE-2025-30698, CVE-2025-30749, CVE-2025-30754, CVE-2025-50059, CVE-2025-5010) (Bug #58529)
  - **rhonabwy** (CVE-2024-25714) (Bug #58389)
  - **squid** (CVE-2023-5824, CVE-2025-54574) (Bug #58539)
  - **sudo** (CVE-2025-32462) (Bug #58440)

- **xorg-server** (CVE-2025-49175, CVE-2025-49176, CVE-2025-49177, CVE-2025-49178, CVE-2025-49179, CVE-2025-49180) (Bug #58437)

- Univention Corporate Server 5.2-3 includes the following updated packages from Debian 12:

  aide catdoc chromium djvulibre ffmpeg gst-plugins-bad1.0 konsole libblock-dev libxml2 mediawiki node-cipher-base nodejs pgpool2 php8.2 qemu redis ring slurm-wlm sope thunderbird trafficserver udisks2 unbound webkit2gtk

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

  asgi-correlation-id (Bug #58421), **nats-py** (Bug #58420), **univention-provisioning-stack-listener** (Bug #58423)

CHAPTER

TWO

DOMAIN SERVICES

2.1 OpenLDAP

- OpenLDAP increased the maximum number of indexed attributes from 128 to 256 (Bug #58443).

2.1.1 Listener/Notifier domain replication

- During the UCS (Univention Corporate Server) domain join process, **`slapd`** fails to start if schema lines exceed 2000 bytes. The issue is resolved by wrapping long `attributeType` and `objectClass` lines at 1500 characters to prevent this failure (Bug #56247).
- Fixed a race condition that could prevent listener modules from initializing properly (Bug #58522).

2.2 LDAP Directory Manager

- The experimental delegative administration feature has been integrated into the UDM (Univention Directory Manager) core library (Bug #58432).
- The primary groups for users and computers are now configurable at the parent container objects where an object is going to be created (Bug #58356).
- Further improvements for the delegative administration feature have been implemented (Bug #58517).
- Clean up references to apps installed on a domain controller or member server when the computer object is removed (Bug #54892).
- Experimental support for delegative administration has been added to the UDM REST API (Bug #58432).

CHAPTER

THREE

UNIVENTION MANAGEMENT CONSOLE

3.1 Univention Management Console server

- The error message for 502/503 HTTP errors for services underneath of `/univention/`, like the **`Guardian`**, has been corrected (Bug #58404).
- Fixed authentication failure lockout functionality for the UMC (Univention Management Console) to properly track and enforce login attempt limits (Bug #57968).

3.2 Univention App Center

- Fixed the directory where the *App Center* stores the cache for the next release during **`univention-app update-check`** (Bug #58240).
- The *App Center* cache is invalidated if the download fails due to network issues to avoid inconsistency in the *App Center* cache (Bug #58469).

3.3 User management

- Deactivate an unnecessary **`systemd`** service when installing the **`Self Service`** app on a Replica Directory Node (Bug #51256).

3.4 Univention Directory Reports

- The creation of reports now evaluates the authorization rules (Bug #58517).

3.5 System diagnostic module

- This update ships the UMC diagnostic plugin `71_samba_memberOf` which checks that the `memberOf` attribute is visible in the output of **`univention-s4search`** and offers possible measures in case that it `memberOf` attribute isn't visible. This update is a follow-up to KB 18673 (Bug #53882).
- The output of the diagnostic module `58_univentionObjectIdentifier` is now more verbose and shows the affected objects (Bug #58446).

3.6 LDAP directory browser

- The experimental delegative administration feature has been integrated into the UDM core library (Bug #58432).
- The primary groups for users and computers are now configurable at the parent container objects where an object is going to be created (Bug #58356).
- The default global search container, for example *"All containers"*, can now be deactivated through the Univention Configuration Registry Variable `directory/manager/web/modules/search/global-search`. If deactivated, you can enable the Univention Configuration Registry Variable `directory/manager/web/modules/search/default-search` to limit searches to module-specific default containers. This improves search performance and result relevance, especially in large environments with many objects (Bug #58418).

CHAPTER

FOUR

UNIVENTION BASE LIBRARIES

- The script **univention-update-univention-object-identifier** now provides a `--dry-run` option (Bug #58446).
- **ldap_setup_index** now checks if number of indexed attributes would exceed maximum number of **lmdb** sub-databases (Bug #58443).
- The primary groups for users and computers are now configurable at the parent container objects where an object is going to be created (Bug #58356).
- The experimental delegative administration feature has been integrated into the UDM core library (Bug #58432).
- Further improvements for the delegative administration feature have been implemented (Bug #58517).

CHAPTER

FIVE

SOFTWARE DEPLOYMENT

- The pre-update script has been updated to run **`univention-prune-kernels`**, in case the Univention Configuration Registry Variable `update52/pruneoldkernel` is enabled, before all the other checks (Bug #58386).
- The *JFrog Artifactory* with authentication return a 403 instead of 401 when authentication is missing. This isn't correct. To solve that problem, a preemptive authentication was added which first tries it with credentials, but then also proceeds if they're URL-encoded (Bug #58371).

CHAPTER

SIX

SYSTEM SERVICES

6.1 SAML

- Add a `--force` flag to **`oidc/rp create`** and **`saml/sp create`** which updates existing Keycloak clients to the configuration given by the command (Bug #58426).
- The command **`univention-keycloak saml-client-nameid-mapper create`** wasn't idempotent and failed with a traceback if the mapper already existed, making it unsuitable for the use in join scripts. This has been fixed (Bug #58544).
- Implement compatibility with Keycloak 26.3.1 authentication flows (Bug #58501).

6.2 Mail services

- The Fetchmail listener module now uses **`systemd`** instead of the **`SysV`** init script `/etc/init.d/fetchmail` (Bug #58532).

6.3 RADIUS

- The log file `/var/log/univention/radius_ntlm_auth.log` is no longer emptied during package updates (Bug #58425).
- In some situations, **`univention-radius-ntlm-auth`** did neither correctly report errors to the **`RADIUS`** server nor logged them. The program has been improved and is now able to intercept these errors and log them to `/var/log/univention/radius_ntlm_auth.log` (Bug #58132).
- The permissions for the log file `/var/log/univention/radius_ntlm_auth.log` weren't set correctly by **`logrotate`**, which caused **`univention-radius-ntlm-auth`** to crash. This update automatically corrects the file permissions and the configuration of **`logrotate`** (Bug #58132).

CHAPTER

SEVEN

SERVICES FOR WINDOWS

7.1 Samba

- Pre-create the AD built-in groups `Pre-Windows 2000 Compatible Access`, `Windows Authorization Access Group`, and `IIS_IUSRS` through UDM in the join script. This is required, because Univention puts those groups on the `connector/s4/mapping/group/ignorelist`, but Univention wants them to be defined with static POSIX IDs across the UCS domain. As a result, these groups are now created with the `hidden` flag, so they don't show up in UMC for new UCS domains. That's okay, because they aren't to be administrated in any way, they just allocate a POSIX ID. This update is a follow-up to KB 18673 (Bug #53882).
- Samba 4.21 had a regression where **`samba-tool domain trust create`** failed to create the trust object. The upstream patch for Samba 4.22 has been ported back to fix this (Bug #58299).

7.2 Univention S4 Connector

- Add the AD built-in groups `Pre-Windows 2000 Compatible Access`, `Windows Authorization Access Group`, and `IIS_IUSRS` to the Univention Configuration Registry Variable `connector/s4/mapping/group/ignorelist`. The first of these groups is relevant to control access to the attribute `memberOf` in Active Directory, for example for `univention-s4search`. By default, it contains the virtual group `Authenticated Users`, but may be configured differently in Samba/AD for security reasons. This update is a follow-up to KB 18673 (Bug #53882).
- Slight adjustments for the experimental delegative administration feature have been done (Bug #58432).

7.3 Univention Active Directory Connection

- Introduced the Univention Configuration Registry Variable `connector/ad/mapping/allow-subtree-ancestors`, which, if enabled, allows the synchronization of ancestors of sub-trees allowed with the Univention Configuration Registry Variables `connector/ad/mapping/allowsubtree/.*/[ad|ucs]`. This can make the management of the selective synchronization of more complex LDAP DIT structures simpler. Additionally, when this new variable is enabled, a re-synchronization with one of the `resync_object_from_*` scripts will handle the re-synchronization of ancestors automatically if necessary (Bug #57979).
- Slight adjustments for the experimental delegative administration feature have been done (Bug #58432).
- In cases where customers chose LDAPS as protocol to bind to Active Directory, by setting the UCR variables `connector/ad/ldap/port=636` and `connector/ad/ldap/ldaps=yes`, the script **`univention-adsearch`** aborted with `NT_STATUS_INVALID_PARAMETER_MIX`. Now it passes the parameters `tls cafile` and `tls crlfile` to **`ldbsearch`** to avoid that error message (Bug #56139).

CHAPTER

EIGHT

OTHER CHANGES

- A new library for delegative administration has been introduced (Bug #58432).

INDEX

B

C

D

E

K

U