univention
be open.

Changelog for Univention Corporate Server (UCS) 5.2-2

Release 5.2-2

Jun 11, 2025

CONTENTS

CHAPTER

ONE

GENERAL

- Univention Corporate Server 5.2-2 includes all security updates issued for UCS (Univention Corporate Server) 5.2-1:
  - **abseil** (CVE-2025-0838) (Bug #58295)
  - **curl** (CVE-2024-11053, CVE-2024-9681, CVE-2025-0167) (Bug #58098)
  - **exim4** (CVE-2025-30232) (Bug #58157)
  - **firefox-esr** (CVE-2024-43097, CVE-2025-1931, CVE-2025-1932, CVE-2025-1933, CVE-2025-1934, CVE-2025-1935, CVE-2025-1936, CVE-2025-1937, CVE-2025-1938, CVE-2025-3028, CVE-2025-3029, CVE-2025-3030, CVE-2025-4083, CVE-2025-4087, CVE-2025-4091, CVE-2025-4093, CVE-2025-4920, CVE-2025-4921) (Bug #58167, Bug #58241, Bug #58289)
  - **freetype** (CVE-2025-27363) (Bug #58105)
  - **gcc-12** (CVE-2023-4039) (Bug #58315)
  - **ghostscript** (CVE-2025-27830, CVE-2025-27831, CVE-2025-27832, CVE-2025-27833, CVE-2025-27834, CVE-2025-27835, CVE-2025-27836) (Bug #58148)
  - **glib2.0** (CVE-2025-3360) (Bug #58292)
  - **glibc** (CVE-2025-0395) (Bug #58112)
  - **imagemagick** (CVE-2025-43965) (Bug #58283)
  - **intel-microcode** (CVE-2023-34440, CVE-2023-43758, CVE-2024-24582, CVE-2024-28047, CVE-2024-28127, CVE-2024-28956, CVE-2024-29214, CVE-2024-31068, CVE-2024-31157, CVE-2024-36293, CVE-2024-37020, CVE-2024-39279, CVE-2024-39355, CVE-2024-43420, CVE-2024-45332, CVE-2025-20012, CVE-2025-20054, CVE-2025-20103, CVE-2025-20623, CVE-2025-24495) (Bug #58108, Bug #58323)
  - **jinja2** (CVE-2024-56201, CVE-2024-56326) (Bug #58099)
  - **krb5** (CVE-2024-26462, CVE-2025-24528) (Bug #58281)
  - **libcap2** (CVE-2025-1390) (Bug #58296)
  - **libxslt** (CVE-2024-55549, CVE-2025-24855) (Bug #58110)
  - **linux** (CVE-2023-52857, CVE-2024-24855, CVE-2024-26596, CVE-2024-26656, CVE-2024-26767, CVE-2024-26982, CVE-2024-27056, CVE-2024-35866, CVE-2024-36908, CVE-2024-38611, CVE-2024-40945, CVE-2024-40973, CVE-2024-42069, CVE-2024-42122, CVE-2024-43831, CVE-2024-45001, CVE-2024-46733, CVE-2024-46742, CVE-2024-46753, CVE-2024-46772, CVE-2024-46774, CVE-2024-46816, CVE-2024-46823, CVE-2024-47726, CVE-2024-47753, CVE-2024-47754, CVE-2024-49989, CVE-2024-50056, CVE-2024-50061, CVE-2024-50063, CVE-2024-50246, CVE-2024-53166, CVE-2024-54458, CVE-2024-56549, CVE-2024-57834, CVE-2024-57973, CVE-2024-57977, CVE-2024-57978, CVE-2024-57979, CVE-2024-57980, CVE-2024-57981, CVE-2024-57986, CVE-2024-57993, CVE-2024-57996, CVE-2024-57997, CVE-2024-57998, CVE-2024-58001, CVE-2024-58002, CVE-2024-58007, CVE-2024-58009, CVE-2024-58010, CVE-2024-58011, CVE-2024-58013, CVE-2024-58014,

CVE-2024-58016, CVE-2024-58017, CVE-2024-58020, CVE-2024-58034, CVE-2024-58051, CVE-2024-58052, CVE-2024-58054, CVE-2024-58055, CVE-2024-58056, CVE-2024-58058, CVE-2024-58061, CVE-2024-58063, CVE-2024-58068, CVE-2024-58069, CVE-2024-58071, CVE-2024-58072, CVE-2024-58076, CVE-2024-58077, CVE-2024-58079, CVE-2024-58080, CVE-2024-58083, CVE-2024-58085, CVE-2024-58086, CVE-2025-21684, CVE-2025-21700, CVE-2025-21701, CVE-2025-21702, CVE-2025-21703, CVE-2025-21704, CVE-2025-21705, CVE-2025-21706, CVE-2025-21707, CVE-2025-21708, CVE-2025-21711, CVE-2025-21715, CVE-2025-21716, CVE-2025-21718, CVE-2025-21719, CVE-2025-21722, CVE-2025-21724, CVE-2025-21725, CVE-2025-21726, CVE-2025-21727, CVE-2025-21728, CVE-2025-21731, CVE-2025-21734, CVE-2025-21735, CVE-2025-21736, CVE-2025-21738, CVE-2025-21744, CVE-2025-21745, CVE-2025-21748, CVE-2025-21749, CVE-2025-21750, CVE-2025-21753, CVE-2025-21756, CVE-2025-21758, CVE-2025-21760, CVE-2025-21761, CVE-2025-21762, CVE-2025-21763, CVE-2025-21764, CVE-2025-21765, CVE-2025-21766, CVE-2025-21767, CVE-2025-21772, CVE-2025-21775, CVE-2025-21776, CVE-2025-21779, CVE-2025-21780, CVE-2025-21781, CVE-2025-21782, CVE-2025-21785, CVE-2025-21787, CVE-2025-21790, CVE-2025-21791, CVE-2025-21792, CVE-2025-21794, CVE-2025-21795, CVE-2025-21796, CVE-2025-21799, CVE-2025-21802, CVE-2025-21804, CVE-2025-21806, CVE-2025-21811, CVE-2025-21812, CVE-2025-21814, CVE-2025-21819, CVE-2025-21820, CVE-2025-21821, CVE-2025-21823, CVE-2025-21826, CVE-2025-21829, CVE-2025-21830, CVE-2025-21832, CVE-2025-21835, CVE-2025-21838, CVE-2025-21853, CVE-2025-21918, CVE-2025-22126, CVE-2025-37838) (Bug #58106, Bug #58197, Bug #58227)

- **linux-signed-amd64** (CVE-2023-52857, CVE-2024-24855, CVE-2024-26656, CVE-2024-26767, CVE-2024-26982, CVE-2024-27056, CVE-2024-35866, CVE-2024-36908, CVE-2024-38611, CVE-2024-40945, CVE-2024-40973, CVE-2024-42069, CVE-2024-42122, CVE-2024-43831, CVE-2024-45001, CVE-2024-46733, CVE-2024-46742, CVE-2024-46753, CVE-2024-46772, CVE-2024-46774, CVE-2024-46816, CVE-2024-46823, CVE-2024-47726, CVE-2024-47753, CVE-2024-47754, CVE-2024-49989, CVE-2024-50056, CVE-2024-50061, CVE-2024-50063, CVE-2024-50246, CVE-2024-53166, CVE-2024-56549, CVE-2024-57977, CVE-2024-58002, CVE-2024-58079, CVE-2025-21684, CVE-2025-21700, CVE-2025-21701, CVE-2025-21702, CVE-2025-21703, CVE-2025-21704, CVE-2025-21756, CVE-2025-21838, CVE-2025-21853, CVE-2025-21918, CVE-2025-22126, CVE-2025-37838) (Bug #58104, Bug #58198, Bug #58227)
- **mariadb** (CVE-2024-21096, CVE-2025-21490) (Bug #58102, Bug #58109)
- **net-tools** (CVE-2025-46836) (Bug #58293)
- **nvidia-graphics-drivers** (CVE-2024-0131, CVE-2024-0147, CVE-2024-0149, CVE-2024-0150, CVE-2024-53869, CVE-2025-23244) (Bug #58290)
- **openjdk-17** (CVE-2025-21587, CVE-2025-30691, CVE-2025-30698) (Bug #58274)
- **openssh** (CVE-2025-32728) (Bug #58297)
- **openssl** (CVE-2024-13176) (Bug #58287)
- **perl** (CVE-2024-56406) (Bug #58194)
- **poppler** (CVE-2023-34872, CVE-2024-56378, CVE-2025-32364, CVE-2025-32365) (Bug #58288)
- **postgresql-15** (CVE-2025-1094, CVE-2025-4207) (Bug #58115, Bug #58291)
- **python-h11** (CVE-2025-43859) (Bug #58298)
- **python3.11** (CVE-2025-0938, CVE-2025-1795) (Bug #58286)
- **shadow** (CVE-2023-29383, CVE-2023-4641) (Bug #58284)
- **sssd** (CVE-2023-3758) (Bug #58107)
- **vim** (CVE-2023-2610, CVE-2023-4738, CVE-2023-4752, CVE-2023-4781, CVE-2023-5344, CVE-2024-22667, CVE-2024-43802, CVE-2024-47814) (Bug #58103)
- **wget** (CVE-2024-38428) (Bug #58111)
- **xz-utils** (CVE-2025-31115) (Bug #58168)

- Univention Corporate Server 5.2-2 includes the following updated packages from Debian 12:

  docker.io fig2dev base-files bash busybox containerd debian-archive-keyring distro-info-data dns-root-data initramfs-tools nvidia-graphics-drivers-tesla qemu rsyslog spamassassin systemd tzdata wireless-regdb xen 389-ds-base atop bup cdebootstrap chkrootkit chromium crowdsec dacite dar dcmtk debian-installer debian-installer-netboot-images debian-ports-archive-keyring debian-security-support dgit djoser dpdk edk2 elpa erlang fossil gensim golang-github-containerd-stargz-snapshotter golang-github-containers-buildah golang-github-openshift-image-builder graphicsmagick haproxy igtf-policy-bundle iptables-netflow jetty9 joblib lemonldap-ng libapache-mod-jk libapache2-mod-auth-openidc libbson-xs-perl libdata-entropy-perl libeconf libpod librabbitmq libreoffice libsub-handlesvia-perl libtar linuxcnc logcheck ltt-control lttng-modules mediawiki mercurial monero mongo-c-driver mozc ndcube network-manager nginx node-axios node-fstream-ignore node-js-sdsl node-postcss node-recast node-redis node-rollup node-send node-serialize-javascript nvidia-graphics-drivers-tesla-535 nvidia-open-gpu-kernel-modules nvidia-settings open-vm-tools openh264 openrazer opensaml opensnitch openvpn php-nesbot-carbon php8.2 phpmyadmin policyd-rate-limit prometheus prometheus-postfix-exporter puma python-pycdlib qtbase-opensource-src rails rapiddisk redis renaissance request-tracker4 request-tracker5 ruby-rack runit-services sash seqan3 simgear skeema skopeo subversion sunpy telegram-desktop thunderbird tomcat10 trafficserver tripwire twitter-bootstrap3 twitter-bootstrap4 user-mode-linux vagrant varnish vips webkit2gtk xmedcon zsh

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

  nvidia-graphics-drivers-tesla-535

CHAPTER

TWO

BASIC SYSTEM SERVICES

2.1 Univention Configuration Registry

2.1.1 Changes to templates and modules

- Bash shell command line completion was not available by default for interactive non-login shells, affecting screen and `sudo` sessions. The UCR template for `/etc/bash.bashrc` has been adjusted to enable command line completion by default for interactive shells (Bug #54717).
- The **`route`** tool from the package is used on some UCS systems for the configuration of additional routes through Univention Configuration Registry Variables. Due to a change in the package dependencies with UCS 5.2-0, the **`net-tools`** package was no longer installed automatically, which meant that these additional routes were no longer set automatically when configuring the network interfaces. The package dependencies have been adjusted accordingly so that this package is now automatically installed again (Bug #58061).
- This update delivers the new command line tool **`univention-lmdb-fragmentation`** that can be used to detect excessive fragmentation in the LMDB databases used in UCS (Bug #58047).

2.2 Other system services

- The allowed machine password length has been increased from 60 to 256 characters (Bug #52575).

CHAPTER

THREE

DOMAIN SERVICES

3.1 OpenLDAP

- When checking for password expiry the **OpenLDAP** overlay module `shdowbind` looks at the LDAP attribute `shadowMax`, which is stored at the user accounts. It treated a value of `0` specially as *"no expiry check needed"*. Univention improved input value validation, because a value of `0` was consider invalid before. This update changes that and it treats it as a normal value. This change became necessary to make the handling of password expiry more consistent on the day of expiry between `pam_unix`, **OpenLDAP** and **Kerberos** (Bug #58048).
- The tool `slapschema` returned an exit status of zero if the last object checked was OK, even if it found problems with previous objects. So it behaved a bit like the `-c` option was given. Now the tool stops on first error unless `-c` is given and returns a non-zero exit code in case a problem is detected on any of the objects checked (Bug #58120).

3.2 LDAP Directory Manager

- First incremental release for new experimental feature delegate administration (Bug #58113).
- Improved performance when removing computer objects in environments with many DNS host records significantly (Bug #58119).
- Attributes containing distinguished names as values were normalized and thus may have differed in string representation from the distinguished names of LDAP objects themselves. This could lead to errors in the UMC (Univention Management Console) not recognizing the correct item in `combobox` widgets. This has been aligned, all data is now written un-normalized (Bug #58261).
- In the experimental feature *"delegative administration"*, administrators can now define writable attributes for UDM (Univention Directory Manager) objects (Bug #58201).
- The PAM module `pam_unix` interprets `(shadowLastChange + shadowMax)` as a date where the password is still valid. For example, with `shadowMax=1` this PAM module considers a password valid during the day after the change. That causes inconsistent behavior when compared to :program:`Kerberos`, where ``krb5PassswordEnd` defines a definite point in time, where the password is considered invalid and UDM sets `krb5PasswordEnd` to the beginning of the day of expiry. `shadowMax` is an LDAP attribute that is added to user accounts during password change and the value is determined by the UDM password history policy applied to the user. UDM now sets `shadowMax` to `(pwhistoryPolicy.expiryInterval -1)` to compensate for the behavior of `pam_unix` and make it more consistent with the behavior of **Kerberos** (Bug #58048).
- UDM hook extension modules could overwrite members of the global Python namespace, possibly leading to trivial conflicts between imported modules. The import of these modules has been adjusted to sandbox their global namespace and selectively import only the intended subclass types (Bug #57630).
- The `univentionObjectIdentifier` UDM property has been added to all UDM modules. It is set to an auto-generated value if none was specified in the create request (Bug #58252, Bug #58318).

- An LDAP equality index is now created for the attribute `univentionObjectIdentifier` (Bug #57393).
- The OpenAPI schema has been adjusted to allow the specification of multiple policies for UCR policies (Bug #57988).

CHAPTER

FOUR

UNIVENTION MANAGEMENT CONSOLE

4.1 Univention Management Console web interface

- The *Tree* widget now correctly encodes its content, effectively removing an cross-site scripting (XSS) attack vector (Bug #49001).
- A syntax check error message didn't properly escape HTML code in XSS attempts on UCR keys (Bug #58279).
- Certain widgets, for example, in the *Users Module*, weren't considered as empty by the frontend although they were. This led to values being sent to backend that should have been ignored. This has been fixed (Bug #58130).
- Improved the styling of the *MultiInput* widget when displaying more than two input fields to enhance UI appearance in the UMC (Bug #58122).

4.2 Univention Portal

- The *Portal* now sanitizes HTML content in tooltips and notifications to prevent cross-site scripting (XSS) vulnerabilities (Bug #58311).
- The server's address is no longer included in the `meta.json` file by default and is now only visible during system setup to prevent information disclosure (Bug #58280).

4.3 Univention Management Console server

- Unused information for un-authenticate user has been removed from the `meta.json` to prevent information disclosures (Bug #54257).
- The server's address is no longer included in the `meta.json` file by default and is now only visible during system setup to prevent information disclosure (Bug #58280).
- Logging of failure reasons when retrieving the `OIDC` access token has been improved (Bug #58114).
- Logging of stack traces is now done with `ERROR` facility and they are additionally logged to the log files of the modules (Bug #46057).
- A configuration option to deactivate checks for `TLS` encrypted connections has been added the *UMC Server* to support using the `SASL` mechanism `OAUTHBEARER` in **`Kubernetes`** environments (Bug #58210).

4.4 Univention App Center

- Applied stricter content sanitization in the App Center to prevent exploitation via Cross-Site Scripting (XSS) and related attack vectors (Bug #58327).

4.5 Modules for system settings / setup wizard

- Relax hostname length limit from 13 to 15 characters (Bug #56128).

4.6 Domain join module

- The scripts **univention-join** and **univention-run-join-scripts** now set the `umask` to `0022` so that customized more restricted settings don't cause problems in join scripts and listener modules (Bug #56634).
- The usage of `chown` has been made future proof to prevent a misleading error message in the join log file (Bug #58033).

4.7 User management

- Administrators can specify trusted hosts to bypass the UMC **self-service** rate limit. This can be done by adding the hosts to the Univention Configuration Registry Variable `umc/self- service/rate-limit/trusted-hosts` (Bug #58214).
- Users can now edit their country in the self service profile view again. The LDAP attribute `c` has been added to the default list of allowed attributes to be changed in the profile view. Since UCS 5.2 the `Country` property corresponds to the LDAP attribute `c` instead of `st` (Bug #57397).
- The **Self-Service** UMC module now attempts to reconnect if its connection to the **PostgreSQL** database is interrupted during fetching of password reset tokens. If the reconnection attempt fails, the connection is re-established on the next request (Bug #58159).

4.8 System diagnostic module

- This update delivers a new diagnostic module `70_lmdb_fragmentation` that can be used to detect excessive fragmentation in the LMDB databases used in UCS (Bug #58047).
- A new script was added: `univention-export-anonymized-ldap` creates an offline copy of the LDAP server. It anonymizes the data with regards to user data such as names, mail addresses, and passwords. Use case is a file that could be used in testing environments, for example, to analyze performance (Bug #58247).

4.9 Policies

- The allowed machine password length has been increased from 27 to 256 characters (Bug #52575).

4.10 Univention Configuration Registry module

- The UMC module didn't properly escape HTML code forcefully injected from the server side in cross-site scripting (XSS) attempts on UCR keys (Bug #58279).

4.11 LDAP directory browser

- The UDM *Grid* widget now correctly encodes its content, effectively removing an cross-site scripting (XSS) attack vector (Bug #49001).
- First incremental release for new experimental feature delegate administration (Bug #58113).
- In the experimental feature *"delegative administration"* one can now define writable attributes for UDM objects (Bug #58201).
- The performance of receiving object representations in UDM HTTP REST API and the UMC module has been improved (Bug #58278).

CHAPTER

FIVE

UNIVENTION BASE LIBRARIES

- The initial objects during the LDAP bootstrapping of new installations now automatically set generated values for `univenitonObjectIdentifier` (Bug #58310).

CHAPTER

SIX

SYSTEM SERVICES

6.1 SAML

- The options `startTls` and `connectionPooling` are incompatible in **`Keycloak`** 26. As of this version, `connectionPooling` will only be activated if `startTls` is deactivated. This is due to underlying limitations with pooling secure (`TLS`) connections (Bug #58183).
- Add `basic` scope as default scope when creating `OIDC` relying party clients (Bug #58254).

6.2 Mail services

6.2.1 IMAP services

- In certain scenarios the `pwdChangeNextLogin` enabled state of users were reset during `IMAP` authentication in the `PAM` stack of dovecot. This is now prevented (Bug #58127).

CHAPTER

SEVEN

SERVICES FOR WINDOWS

7.1 Univention S4 Connector

- The PAM module `pam_unix` interprets `(shadowLastChange + shadowMax)` as a date where the password is still valid. For example, with `shadowMax=1` this PAM module considers a password valid during the day after the change. That causes inconsistent behavior when compared to :program:`Kerberos`, where ``krb5PasswordEnd`` defines a definite point in time, where the password is considered invalid and UDM sets `krb5PasswordEnd` to the beginning of the day of expiry. `shadowMax` is an LDAP attribute that is added to user accounts during password change and the value is determined by the UDM password history policy applied to the user. UDM now sets `shadowMax` to `(pwhistoryPolicy.expiryInterval -1)` to compensate for the behavior of `pam_unix` and make it more consistent with the behavior of **Kerberos** (Bug #58048).

7.2 Univention Active Directory Connection

- The PAM module `pam_unix` interprets `(shadowLastChange + shadowMax)` as a date where the password is still valid. For example, with `shadowMax=1` this PAM module considers a password valid during the day after the change. That causes inconsistent behavior when compared to :program:`Kerberos`, where ``krb5PasswordEnd`` defines a definite point in time, where the password is considered invalid and UDM sets `krb5PasswordEnd` to the beginning of the day of expiry. `shadowMax` is an LDAP attribute that is added to user accounts during password change and the value is determined by the UDM password history policy applied to the user. UDM now sets `shadowMax` to `(pwhistoryPolicy.expiryInterval -1)` to compensate for the behavior of `pam_unix` and make it more consistent with the behavior of **Kerberos**. The **AD-Connector** has been adjusted accordingly (Bug #58048).

CHAPTER

EIGHT

OTHER CHANGES

- A configuration option to deactivate checks for `TLS` encrypted connections has been added to support using the `SASL` mechanism `OAUTHBEARER` in **`Kubernetes`** environments (Bug #58210).
- A segmentation fault is prevented if the `JWKS` file for the OpenID Connect provider is larger than 8192 bytes (Bug #57508).

INDEX

B

C

E

U