univention
be open.

Changelog for Univention Corporate Server (UCS) 5.2-6

Release 5.2-6

Jun 16, 2026

CONTENTS

CHAPTER

ONE

GENERAL

- Univention Corporate Server 5.2-6 includes all security updates issued for UCS 5.2-5:
  - **apache2** (CVE-2026-23918, CVE-2026-24072, CVE-2026-29169, CVE-2026-33006, CVE-2026-33007, CVE-2026-33523, CVE-2026-33857, CVE-2026-34032, CVE-2026-34059) (Bug #59264)
  - **bind9** (CVE-2026-1519, CVE-2026-3039, CVE-2026-3592, CVE-2026-5946, CVE-2026-5950) (Bug #59152, Bug #59432)
  - **busybox** (CVE-2022-48174, CVE-2023-42363, CVE-2023-42364, CVE-2023-42365) (Bug #59310)
  - **containerd** (CVE-2025-64329) (Bug #59292)
  - **dovecot** (CVE-2025-59031, CVE-2025-59032, CVE-2026-0394, CVE-2026-27855, CVE-2026-27856, CVE-2026-27857, CVE-2026-27858, CVE-2026-27859, CVE-2026-33603, CVE-2026-40016, CVE-2026-40020, CVE-2026-42006) (Bug #59168, Bug #59244, Bug #59309, Bug #59446)
  - **dpkg** (CVE-2025-6297, CVE-2026-2219) (Bug #59293)
  - **exim4** (CVE-2026-40684, CVE-2026-40685, CVE-2026-40686, CVE-2026-40687, CVE-2026-45185) (Bug #59296)
  - **firefox-esr** (CVE-2025-59375, CVE-2026-2447, CVE-2026-2757, CVE-2026-2758, CVE-2026-2759, CVE-2026-2760, CVE-2026-2761, CVE-2026-2762, CVE-2026-2763, CVE-2026-2764, CVE-2026-2765, CVE-2026-2766, CVE-2026-2767, CVE-2026-2768, CVE-2026-2769, CVE-2026-2770, CVE-2026-2771, CVE-2026-2772, CVE-2026-2773, CVE-2026-2774, CVE-2026-2775, CVE-2026-2777, CVE-2026-2778, CVE-2026-2779, CVE-2026-2780, CVE-2026-2781, CVE-2026-2782, CVE-2026-2783, CVE-2026-2784, CVE-2026-2785, CVE-2026-2786, CVE-2026-2787, CVE-2026-2788, CVE-2026-2789, CVE-2026-2790, CVE-2026-2791, CVE-2026-2792, CVE-2026-2793, CVE-2026-4684, CVE-2026-4685, CVE-2026-4686, CVE-2026-4687, CVE-2026-4688, CVE-2026-4689, CVE-2026-4690, CVE-2026-4691, CVE-2026-4692, CVE-2026-4693, CVE-2026-4694, CVE-2026-4695, CVE-2026-4696, CVE-2026-4697, CVE-2026-4698, CVE-2026-4699, CVE-2026-4700, CVE-2026-4701, CVE-2026-4702, CVE-2026-4704, CVE-2026-4705, CVE-2026-4706, CVE-2026-4707, CVE-2026-4708, CVE-2026-4709, CVE-2026-4710, CVE-2026-4713, CVE-2026-4714, CVE-2026-4715, CVE-2026-4716, CVE-2026-4717, CVE-2026-4718, CVE-2026-4719, CVE-2026-4720, CVE-2026-4721, CVE-2026-5731, CVE-2026-5732, CVE-2026-5734, CVE-2026-6746, CVE-2026-6747, CVE-2026-6748, CVE-2026-6749, CVE-2026-6750, CVE-2026-6751, CVE-2026-6752, CVE-2026-6753, CVE-2026-6754, CVE-2026-6757, CVE-2026-6761, CVE-2026-6762, CVE-2026-6763, CVE-2026-6764, CVE-2026-6765, CVE-2026-6766, CVE-2026-6767, CVE-2026-6769, CVE-2026-6770, CVE-2026-6771, CVE-2026-6772, CVE-2026-6776, CVE-2026-6785, CVE-2026-6786, CVE-2026-7320, CVE-2026-7321, CVE-2026-7322, CVE-2026-7323, CVE-2026-8090, CVE-2026-8092, CVE-2026-8094, CVE-2026-8388, CVE-2026-8391, CVE-2026-8401, CVE-2026-8946, CVE-2026-8947, CVE-2026-8950, CVE-2026-8953, CVE-2026-8954, CVE-2026-8955, CVE-2026-8956, CVE-2026-8957, CVE-2026-8958, CVE-2026-8961, CVE-2026-8962, CVE-2026-8968, CVE-2026-8970, CVE-2026-8974,

CVE-2026-8975) (Bug #59126, Bug #59154, Bug #59181, Bug #59227, Bug #59246, Bug #59270, Bug #59430)

- **gdk-pixbuf** (CVE-2026-5201) (Bug #59182)
- **glib2.0** (CVE-2026-0988, CVE-2026-1484, CVE-2026-1485, CVE-2026-1489) (Bug #59306)
- **glibc** (CVE-2025-15281, CVE-2026-0861, CVE-2026-0915, CVE-2026-4046, CVE-2026-4437, CVE-2026-4438) (Bug #59294)
- **gnutls28** (CVE-2026-33845, CVE-2026-33846, CVE-2026-3832, CVE-2026-3833, CVE-2026-42009, CVE-2026-42010, CVE-2026-42011, CVE-2026-42012, CVE-2026-42013, CVE-2026-42014, CVE-2026-42015, CVE-2026-5260, CVE-2026-5419) (Bug #59437)
- **grub-efi-amd64-signed** (CVE-2024-45774, CVE-2024-45775, CVE-2024-45776, CVE-2024-45777, CVE-2024-45778, CVE-2024-45779, CVE-2024-45780, CVE-2024-45781, CVE-2024-45782, CVE-2024-45783, CVE-2025-0622, CVE-2025-0624, CVE-2025-0677, CVE-2025-0678, CVE-2025-0684, CVE-2025-0685, CVE-2025-0686, CVE-2025-0689, CVE-2025-0690, CVE-2025-1118, CVE-2025-1125) (Bug #59290)
- **grub2** (CVE-2024-45774, CVE-2024-45775, CVE-2024-45776, CVE-2024-45777, CVE-2024-45778, CVE-2024-45779, CVE-2024-45780, CVE-2024-45781, CVE-2024-45782, CVE-2024-45783, CVE-2025-0622, CVE-2025-0624, CVE-2025-0677, CVE-2025-0678, CVE-2025-0684, CVE-2025-0685, CVE-2025-0686, CVE-2025-0689, CVE-2025-0690, CVE-2025-1118, CVE-2025-1125) (Bug #59290)
- **haveged** (CVE-2026-41054) (Bug #59431)
- **imagemagick** (CVE-2026-24481, CVE-2026-24484, CVE-2026-24485, CVE-2026-25576, CVE-2026-25638, CVE-2026-25795, CVE-2026-25796, CVE-2026-25797, CVE-2026-25798, CVE-2026-25799, CVE-2026-25897, CVE-2026-25898, CVE-2026-25965, CVE-2026-25968, CVE-2026-25970, CVE-2026-25971, CVE-2026-25982, CVE-2026-25983, CVE-2026-25985, CVE-2026-25986, CVE-2026-25987, CVE-2026-25988, CVE-2026-25989, CVE-2026-26066, CVE-2026-26283, CVE-2026-26284, CVE-2026-26983, CVE-2026-27798, CVE-2026-27799, CVE-2026-28494, CVE-2026-28686, CVE-2026-28687, CVE-2026-28688, CVE-2026-28689, CVE-2026-28690, CVE-2026-28691, CVE-2026-28692, CVE-2026-28693, CVE-2026-30883, CVE-2026-30936, CVE-2026-30937, CVE-2026-31853, CVE-2026-32259, CVE-2026-32636, CVE-2026-33535, CVE-2026-33536, CVE-2026-33899, CVE-2026-33900, CVE-2026-33901, CVE-2026-33905, CVE-2026-33908, CVE-2026-34238, CVE-2026-40310, CVE-2026-40311, CVE-2026-42050, CVE-2026-42326, CVE-2026-45031, CVE-2026-45359, CVE-2026-45624, CVE-2026-45664, CVE-2026-46520, CVE-2026-46521, CVE-2026-46522, CVE-2026-46523, CVE-2026-46559, CVE-2026-46692, CVE-2026-46693, CVE-2026-47165, CVE-2026-47166) (Bug #59125, Bug #59201, Bug #59248, Bug #59448)
- **inetutils** (CVE-2026-24061, CVE-2026-28372, CVE-2026-32746, CVE-2026-32772) (Bug #59167)
- **krb5** (CVE-2026-40355, CVE-2026-40356) (Bug #59428)
- **lcms2** (CVE-2026-41254) (Bug #59271)
- **libarchive** (CVE-2025-5918, CVE-2026-4111, CVE-2026-4424, CVE-2026-4426, CVE-2026-5121) (Bug #59305)
- **libcap2** (CVE-2026-4878) (Bug #59316)
- **libexif** (CVE-2026-32775, CVE-2026-40385, CVE-2026-40386) (Bug #59287)
- **libgcrypt20** (CVE-2026-41989) (Bug #59438)
- **libnet-cidr-lite-perl** (CVE-2026-40198, CVE-2026-40199) (Bug #59308)
- **libpng1.6** (CVE-2026-33416, CVE-2026-33636, CVE-2026-34757) (Bug #59165, Bug #59268)
- **libxml-parser-perl** (CVE-2006-10002, CVE-2006-10003) (Bug #59153)
- **linux** (CVE-2023-53228, CVE-2023-53424, CVE-2023-53510, CVE-2023-53545, CVE-2024-26822, CVE-2024-47736, CVE-2024-47809, CVE-2024-49998, CVE-2024-50298,

CVE-2024-56719, CVE-2024-57895, CVE-2025-21676, CVE-2025-21682, CVE-2025-22026, CVE-2025-23155, CVE-2025-37786, CVE-2025-37920, CVE-2025-37945, CVE-2025-37980, CVE-2025-38105, CVE-2025-38162, CVE-2025-38192, CVE-2025-38201, CVE-2025-38250, CVE-2025-38303, CVE-2025-38436, CVE-2025-38617, CVE-2025-38626, CVE-2025-38643, CVE-2025-38659, CVE-2025-38704, CVE-2025-39748, CVE-2025-39763, CVE-2025-39764, CVE-2025-39863, CVE-2025-40005, CVE-2025-40016, CVE-2025-40082, CVE-2025-40135, CVE-2025-40219, CVE-2025-40242, CVE-2025-40251, CVE-2025-40261, CVE-2025-40358, CVE-2025-68206, CVE-2025-68239, CVE-2025-68265, CVE-2025-68358, CVE-2025-71067, CVE-2025-71089, CVE-2025-71144, CVE-2025-71161, CVE-2025-71221, CVE-2025-71232, CVE-2025-71233, CVE-2025-71235, CVE-2025-71236, CVE-2025-71237, CVE-2025-71265, CVE-2025-71266, CVE-2025-71267, CVE-2025-71269, CVE-2026-23100, CVE-2026-23111, CVE-2026-23112, CVE-2026-23113, CVE-2026-23141, CVE-2026-23154, CVE-2026-23157, CVE-2026-23169, CVE-2026-23204, CVE-2026-23220, CVE-2026-23221, CVE-2026-23222, CVE-2026-23227, CVE-2026-23228, CVE-2026-23229, CVE-2026-23230, CVE-2026-23231, CVE-2026-23242, CVE-2026-23243, CVE-2026-23245, CVE-2026-23253, CVE-2026-23270, CVE-2026-23271, CVE-2026-23273, CVE-2026-23274, CVE-2026-23277, CVE-2026-23279, CVE-2026-23281, CVE-2026-23284, CVE-2026-23286, CVE-2026-23287, CVE-2026-23289, CVE-2026-23290, CVE-2026-23291, CVE-2026-23292, CVE-2026-23293, CVE-2026-23296, CVE-2026-23298, CVE-2026-23300, CVE-2026-23303, CVE-2026-23304, CVE-2026-23306, CVE-2026-23307, CVE-2026-23309, CVE-2026-23312, CVE-2026-23315, CVE-2026-23317, CVE-2026-23318, CVE-2026-23319, CVE-2026-23321, CVE-2026-23324, CVE-2026-23335, CVE-2026-23336, CVE-2026-23339, CVE-2026-23340, CVE-2026-23343, CVE-2026-23351, CVE-2026-23352, CVE-2026-23356, CVE-2026-23357, CVE-2026-23359, CVE-2026-23360, CVE-2026-23362, CVE-2026-23364, CVE-2026-23365, CVE-2026-23367, CVE-2026-23368, CVE-2026-23370, CVE-2026-23372, CVE-2026-23378, CVE-2026-23379, CVE-2026-23381, CVE-2026-23382, CVE-2026-23388, CVE-2026-23391, CVE-2026-23392, CVE-2026-23395, CVE-2026-23396, CVE-2026-23397, CVE-2026-23398, CVE-2026-23401, CVE-2026-23414, CVE-2026-23420, CVE-2026-23422, CVE-2026-23426, CVE-2026-23428, CVE-2026-23434, CVE-2026-23438, CVE-2026-23439, CVE-2026-23446, CVE-2026-23449, CVE-2026-23450, CVE-2026-23452, CVE-2026-23454, CVE-2026-23455, CVE-2026-23456, CVE-2026-23457, CVE-2026-23458, CVE-2026-23460, CVE-2026-23462, CVE-2026-23463, CVE-2026-23474, CVE-2026-23475, CVE-2026-31389, CVE-2026-31391, CVE-2026-31392, CVE-2026-31393, CVE-2026-31396, CVE-2026-31399, CVE-2026-31400, CVE-2026-31402, CVE-2026-31403, CVE-2026-31405, CVE-2026-31408, CVE-2026-31409, CVE-2026-31411, CVE-2026-31412, CVE-2026-31414, CVE-2026-31415, CVE-2026-31416, CVE-2026-31417, CVE-2026-31418, CVE-2026-31421, CVE-2026-31422, CVE-2026-31423, CVE-2026-31424, CVE-2026-31425, CVE-2026-31426, CVE-2026-31427, CVE-2026-31428, CVE-2026-31431, CVE-2026-31433, CVE-2026-31434, CVE-2026-31441, CVE-2026-31446, CVE-2026-31447, CVE-2026-31448, CVE-2026-31450, CVE-2026-31452, CVE-2026-31453, CVE-2026-31454, CVE-2026-31455, CVE-2026-31464, CVE-2026-31466, CVE-2026-31467, CVE-2026-31469, CVE-2026-31473, CVE-2026-31476, CVE-2026-31477, CVE-2026-31478, CVE-2026-31480, CVE-2026-31483, CVE-2026-31485, CVE-2026-31492, CVE-2026-31494, CVE-2026-31495, CVE-2026-31496, CVE-2026-31497, CVE-2026-31498, CVE-2026-31503, CVE-2026-31504, CVE-2026-31507, CVE-2026-31508, CVE-2026-31509, CVE-2026-31510, CVE-2026-31512, CVE-2026-31515, CVE-2026-31518, CVE-2026-31519, CVE-2026-31520, CVE-2026-31521, CVE-2026-31522, CVE-2026-31523, CVE-2026-31524, CVE-2026-31533, CVE-2026-31540, CVE-2026-31545, CVE-2026-31546, CVE-2026-31548, CVE-2026-31549, CVE-2026-31550, CVE-2026-31551, CVE-2026-31552, CVE-2026-31555, CVE-2026-31563, CVE-2026-31565, CVE-2026-31566, CVE-2026-31570, CVE-2026-31628, CVE-2026-31634, CVE-2026-31649, CVE-2026-31651, CVE-2026-31656, CVE-2026-31657, CVE-2026-31658, CVE-2026-31659, CVE-2026-31660, CVE-2026-31661, CVE-2026-31662, CVE-2026-31664, CVE-2026-31665, CVE-2026-31667, CVE-2026-31668, CVE-2026-31669, CVE-2026-31670, CVE-2026-31671, CVE-2026-31672, CVE-2026-31674, CVE-2026-31678, CVE-2026-31679, CVE-2026-31680, CVE-2026-31682, CVE-2026-31683, CVE-2026-31689, CVE-2026-31695, CVE-2026-31720, CVE-2026-31721, CVE-2026-31726, CVE-2026-31728, CVE-2026-31737, CVE-2026-31738, CVE-2026-31747, CVE-2026-31748, CVE-2026-31749, CVE-2026-31751, CVE-2026-31752, CVE-2026-31754, CVE-2026-31755, CVE-2026-31756, CVE-2026-31758, CVE-2026-31759, CVE-2026-31761, CVE-2026-31762, CVE-2026-31763, CVE-2026-31768, CVE-2026-31770, CVE-2026-31773,

CVE-2026-31778, CVE-2026-31779, CVE-2026-31780, CVE-2026-31781, CVE-2026-31786, CVE-2026-31787, CVE-2026-31788, CVE-2026-43011, CVE-2026-43013, CVE-2026-43014, CVE-2026-43015, CVE-2026-43017, CVE-2026-43018, CVE-2026-43020, CVE-2026-43023, CVE-2026-43024, CVE-2026-43025, CVE-2026-43026, CVE-2026-43027, CVE-2026-43028, CVE-2026-43030, CVE-2026-43032, CVE-2026-43033, CVE-2026-43035, CVE-2026-43037, CVE-2026-43038, CVE-2026-43040, CVE-2026-43041, CVE-2026-43043, CVE-2026-43046, CVE-2026-43047, CVE-2026-43050, CVE-2026-43051, CVE-2026-43054, CVE-2026-43057, CVE-2026-43284, CVE-2026-43500, CVE-2026-43503, CVE-2026-46300, CVE-2026-46333) (Bug #59124, Bug #59245, Bug #59279, Bug #59320, Bug #59447)

- **linux-signed-amd64** (CVE-2023-53228, CVE-2023-53424, CVE-2023-53510, CVE-2023-53545, CVE-2024-26822, CVE-2024-47736, CVE-2024-47809, CVE-2024-49998, CVE-2024-50298, CVE-2024-56719, CVE-2024-57895, CVE-2025-21676, CVE-2025-21682, CVE-2025-22026, CVE-2025-23155, CVE-2025-37786, CVE-2025-37920, CVE-2025-37945, CVE-2025-38105, CVE-2025-38162, CVE-2025-38192, CVE-2025-38201, CVE-2025-38250, CVE-2025-38303, CVE-2025-38643, CVE-2025-38659, CVE-2025-38704, CVE-2025-39748, CVE-2025-39763, CVE-2025-39764, CVE-2025-39863, CVE-2025-40005, CVE-2025-40082, CVE-2025-40135, CVE-2025-40242, CVE-2025-40251, CVE-2025-40261, CVE-2025-68206, CVE-2025-68239, CVE-2025-68265, CVE-2025-68358, CVE-2025-71067, CVE-2025-71089, CVE-2025-71144, CVE-2025-71161, CVE-2025-71221, CVE-2025-71232, CVE-2025-71233, CVE-2025-71235, CVE-2025-71236, CVE-2025-71237, CVE-2025-71269, CVE-2026-23100, CVE-2026-23111, CVE-2026-23112, CVE-2026-23113, CVE-2026-23141, CVE-2026-23154, CVE-2026-23157, CVE-2026-23169, CVE-2026-23204, CVE-2026-23220, CVE-2026-23221, CVE-2026-23222, CVE-2026-23227, CVE-2026-23228, CVE-2026-23229, CVE-2026-23230, CVE-2026-23231, CVE-2026-23245, CVE-2026-23253, CVE-2026-23270, CVE-2026-23274, CVE-2026-23277, CVE-2026-23279, CVE-2026-23281, CVE-2026-23284, CVE-2026-23286, CVE-2026-23287, CVE-2026-23290, CVE-2026-23291, CVE-2026-23292, CVE-2026-23293, CVE-2026-23296, CVE-2026-23298, CVE-2026-23300, CVE-2026-23303, CVE-2026-23304, CVE-2026-23306, CVE-2026-23309, CVE-2026-23312, CVE-2026-23315, CVE-2026-23317, CVE-2026-23318, CVE-2026-23319, CVE-2026-23324, CVE-2026-23335, CVE-2026-23336, CVE-2026-23339, CVE-2026-23343, CVE-2026-23351, CVE-2026-23352, CVE-2026-23356, CVE-2026-23357, CVE-2026-23359, CVE-2026-23360, CVE-2026-23362, CVE-2026-23364, CVE-2026-23365, CVE-2026-23367, CVE-2026-23368, CVE-2026-23370, CVE-2026-23372, CVE-2026-23378, CVE-2026-23379, CVE-2026-23381, CVE-2026-23382, CVE-2026-23388, CVE-2026-23391, CVE-2026-23392, CVE-2026-23395, CVE-2026-23396, CVE-2026-23397, CVE-2026-23398, CVE-2026-23401, CVE-2026-23414, CVE-2026-31431, CVE-2026-31628, CVE-2026-31786, CVE-2026-31787, CVE-2026-31788, CVE-2026-43284, CVE-2026-43500, CVE-2026-43503, CVE-2026-46300, CVE-2026-46333) (Bug #59124, Bug #59245, Bug #59279, Bug #59320, Bug #59447)
- **nghttp2** (CVE-2026-27135) (Bug #59295)
- **nss** (CVE-2026-2781) (Bug #59123)
- **ntfs-3g** (CVE-2026-40706) (Bug #59228)
- **openjdk-17** (CVE-2026-21925, CVE-2026-21932, CVE-2026-21933, CVE-2026-21945, CVE-2026-22007, CVE-2026-22013, CVE-2026-22016, CVE-2026-22018, CVE-2026-22021, CVE-2026-23865, CVE-2026-34268, CVE-2026-34282) (Bug #59247)
- **openjpeg2** (CVE-2026-6192) (Bug #59314)
- **openssh** (CVE-2025-61984, CVE-2025-61985, CVE-2026-3497, CVE-2026-35385, CVE-2026-35386, CVE-2026-35387, CVE-2026-35388, CVE-2026-35414) (Bug #59184, Bug #59288)
- **openssl** (CVE-2026-28387, CVE-2026-28388, CVE-2026-28389, CVE-2026-28390, CVE-2026-31789, CVE-2026-31790) (Bug #59185, Bug #59318)
- **postgresql-15** (CVE-2026-2006, CVE-2026-6472, CVE-2026-6473, CVE-2026-6474, CVE-2026-6475, CVE-2026-6477, CVE-2026-6478, CVE-2026-6479, CVE-2026-6637) (Bug #59297)

- **pyasn1** (CVE-2026-30922) (Bug #59164)
- **pyjwt** (CVE-2026-32597) (Bug #59269)
- **python-ldap** (CVE-2025-61911, CVE-2025-61912) (Bug #59106)
- **python-tornado** (CVE-2025-67724, CVE-2025-67725, CVE-2025-67726) (Bug #59166)
- **python3.11** (CVE-2025-11468, CVE-2025-12084, CVE-2025-13836, CVE-2025-13837, CVE-2025-15282, CVE-2025-4516, CVE-2025-6069, CVE-2025-6075, CVE-2025-8194, CVE-2025-8291, CVE-2026-0672, CVE-2026-0865, CVE-2026-1299) (Bug #59286)
- **rsync** (CVE-2026-29518, CVE-2026-43617, CVE-2026-43618, CVE-2026-43619, CVE-2026-43620) (Bug #59436)
- **samba** (CVE-2026-1933, CVE-2026-2340, CVE-2026-3012, CVE-2026-3238, CVE-2026-4408, CVE-2026-4480) (Bug #59161, Bug #59259)
- **sed** (CVE-2026-5958) (Bug #59315)
- **sudo** (CVE-2026-35535) (Bug #59313)
- **systemd** (CVE-2026-29111, CVE-2026-40225, CVE-2026-40226, CVE-2026-4105) (Bug #59311)
- **tiff** (CVE-2026-4775) (Bug #59183)
- **xorg-server** (CVE-2026-33999, CVE-2026-34000, CVE-2026-34001, CVE-2026-34002, CVE-2026-34003) (Bug #59312)
- **zvbi** (CVE-2025-2173, CVE-2025-2174, CVE-2025-2175, CVE-2025-2176, CVE-2025-2177) (Bug #59307)

- Univention Corporate Server 5.2-6 includes the following updated packages from Debian 12.14:
  - **7zip**
  - **arduino-core-avr**
  - **augeas**
  - **awstats**
  - **bash**
  - **base-files**
  - **c3p0**
  - **calibre**
  - **cdebootstrap**
  - **chkrootkit**
  - **chromium**
  - **chrony**
  - **composer**
  - **corosync**
  - **dar**
  - **debian-installer-netboot-images**
  - **debsig-verify**
  - **deets**
  - **distro-info-data**
  - **dnsmasq**
  - **docker.io**

- **erlang**
- **evince**
- **exim4**
- **ffmpeg**
- **flatpak**
- **fonttools**
- **gimp**
- **glance**
- **gnuais**
- **golang-github-containerd-stargz-snapshotter**
- **golang-github-containers-buildah**
- **golang-github-openshift-imagebuilder**
- **gpsd**
- **gsasl**
- **gst-plugins-bad1.0**
- **gst-plugins-base1.0**
- **gst-plugins-ugly1.0**
- **gvfs**
- **jtreg7**
- **kdenlive**
- **kissfft**
- **kpackage**
- **lemonldap-ng**
- **libpod**
- **libreoffice**
- **libreoffice-texmaths**
- **libuev**
- **libvncserver**
- **libxml-security-java**
- **libxslt**
- **libyaml-syck-perl**
- **lxc**
- **lxd**
- **mapserver**
- **mediawiki**
- **modsecurity-crs**
- **mongo-c-driver**
- **mupdf**
- **nagios4**

- **netty**
- **nginx**
- **ngtcp2**
- **node-shell-quote**
- **nodejs**
- **opam**
- **openvpn**
- **p7zip**
- **p7zip-rar**
- **packagekit**
- **php-dompdf**
- **php-league-commonmark**
- **php-phpseclib**
- **php-phpseclib3**
- **php-symfony-contracts**
- **php-twig**
- **php8.2**
- **phpseclib**
- **plastimatch**
- **postorius**
- **proftpd-dfsg**
- **prosody**
- **pymupdf**
- **python-authlib**
- **qemu**
- **redis**
- **request-tracker5**
- **roundcube**
- **ruby-rack**
- **sash**
- **simpleeval**
- **sioyek**
- **skeema**
- **snapd**
- **starlette**
- **strongswan**
- **supermin**
- **swupdate**
- **symfony**

- **taglib**
- **thunderbird**
- **tor**
- **tpm2-pkcs11**
- **trafficserver**
- **tripwire**
- **tzdata**
- **user-mode-linux**
- **vips**
- **webkit2gtk**
- **wireless-regdb**
- **wireshark**
- **xdg-dbus-proxy**
- **yelp**
- **zsh**

CHAPTER

TWO

BASIC SYSTEM SERVICES

2.1 Other system services

- The `univentionObjectIdentifier` is now set for all DNS, DHCP and license objects (Bug #58384).
- The counts of licensed users, servers, and managed clients are now cached on the license object through a cron job. The cached numbers improve the performance during UMC startup (Bug #59060).
- License initialization no longer resets the log level to `ERROR`. As a result, the UMC UDM modules keep their log messages (Bug #38735).
- The GPG signing key for UCS 5.3 has been added to the `univention-archive-key` package (Bug #59471).

CHAPTER

THREE

DOMAIN SERVICES

- The `univention-telemetry` package has been added as a recommended dependency for **`univention-server`** (Bug #59235).

3.1 OpenLDAP

3.1.1 Listener/Notifier domain replication

- The syntax of DNs is now validated in `univention-replicate-one` (Bug #33898).

3.2 LDAP Directory Manager

- The `univentionObjectIdentifier` is now set for all DNS, DHCP and license objects (Bug #58384).
- A new extended attribute hook mechanism has been added, which runs before and after moving an object (Bug #59111).
- The counts of licensed users, servers, and managed clients are now cached on the license object through a cron job. The cached numbers improve the performance during UMC startup. Additionally, the obsolete License Version 1, Free For Personal Use Edition, Univention Corporate Clients, GPL License, Desktop Virtualization Services has been removed from the license evaluation (Bug #59060).
- Searching in UMC modules now returns correct results regardless of whether automatic substring search is turned on or off. Previously, when substring search was deactivated, the global search and the standard properties filter didn't return results, due to a broken LDAP filter (Bug #59104).
- The license interface has been extended to use the `entryUUID` of the license as fallback key ID (Bug #59176).
- The hooks API has been extended to support `map()` and `unmap()` methods for extended attributes (Bug #59150).
- The license cache is now also evaluated for unlimited licenses (Bug #59215).
- The `univentionObjectIdentifier` and other technical information about LDAP operational attributes has been added to the advanced settings tab of all UDM modules (Bug #59217).
- The `unixTime` UDM syntax is now compatible with UDM HTTP REST API (Bug #58211).
- The `users/contact` UDM module now lets you set the `cn` property explicitly, so you can create objects deterministically. The UDM CLI now also displays the correct new DN after moving an object (Bug #59281).
- The UDM HTTP REST API now returns HTTP 500 (Internal Server Error) instead of HTTP 400 (Bad Request) when concurrent modifications to the same LDAP object cause `Type or value exists` or `No such attribute` errors. This makes the error transparent to clients and allows them to retry the request (Bug #58804).
- The UDM HTTP REST API now exposes a Prometheus-compatible metrics endpoint at `/univention/udm/-/metrics`. It provides the total number of active users, the licensed user limit, and platform/version information for UCS and Nubus for Kubernetes. All metrics include a domain label and a stable domain identifier derived from the license key. The endpoint is restricted to authorized users (Bug #59176).

- The Nubus Prometheus metrics are now consistently prefixed with `nubus_`, ensuring clearer namespace separation and easier identification in monitoring and alerting configurations. The Nubus Prometheus metrics `nubus_users_user_total` and `nubus_settings_license_users_limit_total` now include the license key as a label, enabling per-license observability (Bug #59231).
- A pre-calculated value for `univentionObjectIdentifier` is now hidden in the object template, as this might be used to create multiple objects (Bug #59217).

CHAPTER

FOUR

UNIVENTION MANAGEMENT CONSOLE

4.1 Univention Management Console web interface

- A regression has been fixed, which was introduced by updating Dojo `dgrid` to version 1.3.3 in UCS 5.2 Erratum 304 and caused the “Select All” checkbox in list views and the tree view in the LDAP directory to malfunction (Bug #59095).
- The `DateTime` widget has been fixed to support all and empty date formats and respect the configured size (Bug #59217).

4.2 Univention Management Console server

- A file descriptor leak caused during PAM authentication through SSS has been fixed (Bug #59220).
- The UMC server no longer accepts smuggled HTTP request headers in `X-UMC-Federated-Account` and `X-UMC-Roles`. These headers handle interprocess communication between the UMC server and UMC module processes when delegative administration is enabled (Bug #59280).

4.3 Univention App Center

- The App Center now avoids allocating Docker Compose network subnets that overlap with host network interfaces, preventing potential routing conflicts (Bug #55073).
- Links in app descriptions and license agreements now open in a new browser tab instead of loading inside the App Center iframe (Bug #57501).

4.4 Domain join module

- The version check in **`univention-join`** used string concatenation with **`awk`** numeric comparison, causing incorrect results for version numbers like 5.0-10 vs 5.0-9. The fix uses **`dpkg --compare-versions`** for correct Debian version ordering (Bug #58212).

4.5 System diagnostic module

- A new diagnostic check warns when the Docker bridge network overlaps with a host network interface, which can cause routing issues (Bug #55073).

4.6 LDAP directory browser

- The underlying library dependencies to handle certificates have been updated from `M2Crypto` and `PyOpenSSL` to `python3-cryptography` to ensure future compatibility and to fix a problem for certificate validity dates after 2050 (Bug #55411).
- The `univentionObjectIdentifier` is now set for all DNS, DHCP and license objects (Bug #58384).

- The counts of licensed users, servers, and managed clients are now cached on the license object through a cron job. The cached numbers improve the performance during UMC startup (Bug #59060).
- UDM now lets you add a property to the layout even when its default value is a function call. All UDM modules now show `univentionObjectIdentifier` and other technical information about LDAP operational attributes on the *Advanced settings* tab (Bug #59217).

CHAPTER

FIVE

UNIVENTION BASE LIBRARIES

- The `univentionObjectIdentifier` is now set for all DNS, DHCP and license objects (Bug #58384).
- The counts of licensed users, servers, and managed clients are now cached on the license object through a cron job. The cached numbers improve the performance during UMC startup (Bug #59060).
- The `crudeoauth` library has been made compatible with modern compilers (Bug #59470).
- The Nagios suidwrapper has been modernized to be compatible with modern compilers (Bug #59469).

CHAPTER

SIX

SOFTWARE DEPLOYMENT

- After a patchlevel update, UDM extensions are now automatically synchronized again to ensure that extensions with version constraints are correctly activated or deactivated for the new UCS version (Bug #59229).

CHAPTER

SEVEN

SYSTEM SERVICES

7.1 SAML

- Fixed a regression introduced in Keycloak 26.6.0 where a change in the component lookup API broke the Kerberos configuration update in the **`univention-keycloak`** script (Bug #59212).
- The package was rebuilt as part of an internal repository migration. This update contains no functional changes (Bug #59234).

7.2 Mail services

- The UDM hooks have been adjusted to be compatible with delegative administration (Bug #59150).

7.2.1 Postfix

- Postfix LDAP group lookups now support the `mailAlternativeAddress` attribute in addition to `mailPrimaryAddress`. This allows UDM groups to receive emails via alternative (alias) addresses (Bug #28692).

CHAPTER

EIGHT

SERVICES FOR WINDOWS

8.1 Samba

- Samba has been updated to version 4.24.2, including the latest security patches, so it's equivalent to 4.24.3 (Bug #59336). For a full list of changes, see the upstream changelogs:
  - Samba 4.22 Features added/changed
  - Samba 4.23 Features added/changed
  - Samba 4.24 Features added/changed
- The Group Policy Management Console was crashing sometimes when modifying the user permissions in the Security tab. Afterwards, the new created ACLs were malformed, which made the policy inaccessible. The code which parses the binary structures sent by the Windows client has been corrected (Bug #59142).
- An uninitialized file descriptor associated with hanging `rpcd spoolss` processes is now initialized (Bug #59160).

8.2 Univention AD Takeover

- The counts of licensed users, servers, and managed clients are now cached on the license object through a cron job. The cached numbers improve the performance during UMC startup (Bug #59060).

8.3 Univention S4 Connector

- The S4 Connector no longer treats stale entries in the connector database as deleted objects in Active Directory. It now verifies that the AD object has `isDeleted=TRUE` before attempting a restore. This change prevents unnecessary restore attempts and synchronization rejects (Bug #59113).
- The S4-Connector now removes the attribute `dNSTombstoned` in Samba/AD if a change for the corresponding DNS object is synchronized from OpenLDAP/UDM (Bug #57174).

8.4 Univention Active Directory Connection

- The **`Active Directory Connection`** no longer treats stale entries in the connector database as deleted objects in Active Directory. It now verifies that the AD object has `isDeleted=TRUE` before attempting a restore. This change prevents unnecessary restore attempts and synchronization rejects (Bug #59113).
- Documentation for the obsolete UCR variable `connector/password/service/encoding.` has been removed (Bug #59128).
- The custom position mapping function of **`Active Directory Connection`** now applies to the object mentioned in the mapping as well (Bug #59200).
- As Microsoft is continuing with the deprecation of NT-hashes, see https://go.microsoft.com/fwlink/?linkid=2344614, the Microsoft update `KB5082063` changed the default value for `DefaultDomainSupportedEncTypes` to allow AES-SHA1 only, which blocks issuing Kerberos tickets with `RC4` hashes. The AD-Connector

now implements the advice by Microsoft to set `msDS-SupportedEncryptionTypes` on a per-account basis during the sync from UCS to Microsoft Active Directory, to allow the Microsoft KDC to make use of the synced NT-hash. As Microsoft doesn't offer an RPC call to pass stronger Kerberos hashes, this workaround is currently necessary. When a password is changed on the Microsoft Active Directory side, **`Active Directory Connection`** removes this setting again, to keep security as high as possible (Bug #58876).

CHAPTER

NINE

OTHER CHANGES

- Password changes through PAM could fail in long-running processes, for example in UMC, with high file descriptor usage. Heimdal Kerberos previously relied on the `select()` API, which can't handle file descriptor values ≥ `FD_SETSIZE` (1024). In such situations, Kerberos communication with the KDC could fail, leading to misleading errors such as `Authentication token manipulation error`. The implementation now uses `poll()`, eliminating this limitation and improving robustness in long-running services (Bug #59145).
- The univention-telemetry package is added, which collects telemetry metrics from UDM HTTP REST API, anonymizes and transforms them to OTLP/JSON format and forwards them to Univention's telemetry receiver. The feature is turned off by default (Bug #59235).

INDEX

B

C

CVE