univention
be open.

Changelog for Univention Corporate Server (UCS) 5.2-7

Release 5.2-7

Sep 22, 2026

CONTENTS

CHAPTER

ONE

GENERAL

- Univention Corporate Server 5.2-7 includes all security updates issued for UCS 5.2-6:
  - **aom** (CVE-2026-56208, CVE-2026-56209, CVE-2026-56210, CVE-2026-56211) (Bug #59908)
  - **apache2** (CVE-2026-29167, CVE-2026-29170, CVE-2026-34355, CVE-2026-34356, CVE-2026-42535, CVE-2026-42536, CVE-2026-43951, CVE-2026-44119, CVE-2026-44185, CVE-2026-44186, CVE-2026-44631, CVE-2026-48913, CVE-2026-49975) (Bug #59500, Bug #59618)
  - **apr-util** (CVE-2025-49506, CVE-2026-32327, CVE-2026-34191, CVE-2026-34501, CVE-2026-34502) (Bug #59749)
  - **bind9** (CVE-2026-10723, CVE-2026-10822, CVE-2026-11331, CVE-2026-11605, CVE-2026-11622, CVE-2026-11721, CVE-2026-12617, CVE-2026-13204, CVE-2026-13321) (Bug #59712)
  - **ceph** (CVE-2024-31884, CVE-2024-47866, CVE-2025-52555) (Bug #59498)
  - **curl** (CVE-2025-10148, CVE-2025-14524, CVE-2025-14819, CVE-2026-3783, CVE-2026-3784, CVE-2026-5773, CVE-2026-7168) (Bug #59615)
  - **expat** (CVE-2026-50219, CVE-2026-56131, CVE-2026-56403, CVE-2026-56404, CVE-2026-56405, CVE-2026-56406, CVE-2026-56407, CVE-2026-56408, CVE-2026-56409, CVE-2026-56410, CVE-2026-56411, CVE-2026-56412, CVE-2026-72522, CVE-2026-76957) (Bug #59911)
  - **firefox-esr** (CVE-2026-12289, CVE-2026-12290, CVE-2026-12291, CVE-2026-12292, CVE-2026-12294, CVE-2026-12295, CVE-2026-12296, CVE-2026-12297, CVE-2026-12298, CVE-2026-12299, CVE-2026-12302, CVE-2026-12304, CVE-2026-12305, CVE-2026-12306, CVE-2026-12307, CVE-2026-12308, CVE-2026-12309, CVE-2026-12310, CVE-2026-12311, CVE-2026-12312, CVE-2026-12313, CVE-2026-12314, CVE-2026-12315, CVE-2026-12324, CVE-2026-12325, CVE-2026-12327, CVE-2026-12328, CVE-2026-12329, CVE-2026-12330, CVE-2026-15718, CVE-2026-15719, CVE-2026-16349, CVE-2026-16350, CVE-2026-16351, CVE-2026-16352, CVE-2026-16353, CVE-2026-16354, CVE-2026-16355, CVE-2026-16356, CVE-2026-16357, CVE-2026-16358, CVE-2026-16359, CVE-2026-16360, CVE-2026-16361, CVE-2026-16362, CVE-2026-16363, CVE-2026-16365, CVE-2026-16368, CVE-2026-16369, CVE-2026-16371, CVE-2026-16374, CVE-2026-16375, CVE-2026-16377, CVE-2026-16379, CVE-2026-16381, CVE-2026-16383, CVE-2026-16387, CVE-2026-16390, CVE-2026-16391, CVE-2026-16396, CVE-2026-16405, CVE-2026-16412, CVE-2026-74934, CVE-2026-74935, CVE-2026-74936, CVE-2026-74939, CVE-2026-74940, CVE-2026-74941, CVE-2026-74942, CVE-2026-74943, CVE-2026-74944, CVE-2026-74945, CVE-2026-74946, CVE-2026-74948, CVE-2026-74949, CVE-2026-74953, CVE-2026-74957, CVE-2026-74959, CVE-2026-74960, CVE-2026-74962, CVE-2026-74963, CVE-2026-74964, CVE-2026-74965, CVE-2026-74967, CVE-2026-74969, CVE-2026-74971, CVE-2026-74972, CVE-2026-74973, CVE-2026-74974, CVE-2026-74976, CVE-2026-74983, CVE-2026-74987, CVE-2026-74990, CVE-2026-75874, CVE-2026-84119, CVE-2026-84120, CVE-2026-84121, CVE-2026-84122, CVE-2026-84124, CVE-2026-84131, CVE-2026-84143, CVE-2026-84145) (Bug #59529, Bug #59681, Bug #59776, Bug #59913)
  - **giflib** (CVE-2026-23868, CVE-2026-26740) (Bug #59622)

- **graphite2** (CVE-2026-50593) (Bug #59610)
- **gsasl** (CVE-2026-48829, CVE-2026-56968) (Bug #59714)
- **hplip** (CVE-2026-8631, CVE-2026-8632) (Bug #59687)
- **imagemagick** (CVE-2026-48733, CVE-2026-48734, CVE-2026-48994, CVE-2026-49218, CVE-2026-53460, CVE-2026-53463, CVE-2026-53466, CVE-2026-53467, CVE-2026-55577, CVE-2026-55594, CVE-2026-55595, CVE-2026-55597, CVE-2026-55628, CVE-2026-56361, CVE-2026-56363, CVE-2026-56365, CVE-2026-56366, CVE-2026-56367, CVE-2026-56368, CVE-2026-56370, CVE-2026-56371, CVE-2026-56373, CVE-2026-56376, CVE-2026-56377, CVE-2026-56378, CVE-2026-61464, CVE-2026-61465, CVE-2026-61857, CVE-2026-61858, CVE-2026-61859, CVE-2026-61860, CVE-2026-61862, CVE-2026-61863, CVE-2026-61864, CVE-2026-61865, CVE-2026-61866, CVE-2026-61868, CVE-2026-61869, CVE-2026-61870, CVE-2026-61872) (Bug #59572, Bug #59657, Bug #59680)
- **libarchive** (CVE-2026-14164, CVE-2026-15028, CVE-2026-16517) (Bug #59907)
- **libbytes-random-secure-perl** (CVE-2026-11625) (Bug #59612)
- **libconfig-inifiles-perl** (CVE-2026-11527) (Bug #59527)
- **libdbi-perl** (CVE-2026-10879, CVE-2026-14380, CVE-2026-14739, CVE-2026-14740, CVE-2026-15043, CVE-2026-15392, CVE-2026-60081, CVE-2026-60082, CVE-2026-73193, CVE-2026-73194, CVE-2026-9698) (Bug #59496, Bug #59910)
- **libgd2** (CVE-2026-9672) (Bug #59747)
- **libhtml-parser-perl** (CVE-2026-8829) (Bug #59608)
- **libhttp-daemon-perl** (CVE-2026-8450) (Bug #59528)
- **libinput** (CVE-2026-50292) (Bug #59501)
- **libnet-cidr-lite-perl** (CVE-2026-45190, CVE-2026-45191) (Bug #59655)
- **libnet-dns-perl** (CVE-2026-64194) (Bug #59860)
- **libnfs** (CVE-2026-53689) (Bug #59653)
- **libssh2** (CVE-2025-15661, CVE-2026-58050, CVE-2026-58051, CVE-2026-66032, CVE-2026-66034, CVE-2026-7598) (Bug #59912)
- **libxfont** (CVE-2026-56001, CVE-2026-56002, CVE-2026-56003) (Bug #59654)
- **libxml-libxml-perl** (CVE-2026-8177) (Bug #59611)
- **libxml2** (CVE-2025-49794, CVE-2025-8732, CVE-2026-0989, CVE-2026-0990, CVE-2026-0992, CVE-2026-1757) (Bug #59621)
- **linux** (CVE-2023-53292, CVE-2023-53989, CVE-2023-54125, CVE-2023-54271, CVE-2023-54322, CVE-2024-27012, CVE-2024-36013, CVE-2024-36922, CVE-2024-53221, CVE-2024-56657, CVE-2025-10263, CVE-2025-21739, CVE-2025-21863, CVE-2025-22105, CVE-2025-23131, CVE-2025-37864, CVE-2025-38349, CVE-2025-38584, CVE-2025-38627, CVE-2025-38710, CVE-2025-39997, CVE-2025-40196, CVE-2025-40347, CVE-2025-68201, CVE-2025-68315, CVE-2025-68823, CVE-2026-23066, CVE-2026-23255, CVE-2026-23272, CVE-2026-23278, CVE-2026-23302, CVE-2026-23310, CVE-2026-23389, CVE-2026-23399, CVE-2026-23442, CVE-2026-23444, CVE-2026-23468, CVE-2026-31407, CVE-2026-31449, CVE-2026-31488, CVE-2026-31489, CVE-2026-31500, CVE-2026-31532, CVE-2026-31576, CVE-2026-31577, CVE-2026-31578, CVE-2026-31580, CVE-2026-31581, CVE-2026-31583, CVE-2026-31585, CVE-2026-31586, CVE-2026-31587, CVE-2026-31588, CVE-2026-31590, CVE-2026-31594, CVE-2026-31595, CVE-2026-31596, CVE-2026-31597, CVE-2026-31598, CVE-2026-31599, CVE-2026-31602, CVE-2026-31603, CVE-2026-31605, CVE-2026-31607, CVE-2026-31610, CVE-2026-31611, CVE-2026-31612, CVE-2026-31613, CVE-2026-31615, CVE-2026-31616, CVE-2026-31617, CVE-2026-31618, CVE-2026-31619, CVE-2026-31622, CVE-2026-31623, CVE-2026-31624, CVE-2026-31625, CVE-2026-31626, CVE-2026-31627, CVE-2026-31629, CVE-2026-31630, CVE-2026-31637, CVE-2026-31642, CVE-2026-31673, CVE-2026-31676, CVE-2026-31681, CVE-2026-31684, CVE-2026-31685, CVE-2026-31686,

CVE-2026-31694, CVE-2026-31696, CVE-2026-31697, CVE-2026-31698, CVE-2026-31699, CVE-2026-31700, CVE-2026-31701, CVE-2026-31702, CVE-2026-31704, CVE-2026-31705, CVE-2026-31708, CVE-2026-31709, CVE-2026-31711, CVE-2026-31712, CVE-2026-31715, CVE-2026-31716, CVE-2026-43052, CVE-2026-43058, CVE-2026-43064, CVE-2026-43071, CVE-2026-43072, CVE-2026-43074, CVE-2026-43075, CVE-2026-43076, CVE-2026-43079, CVE-2026-43080, CVE-2026-43085, CVE-2026-43089, CVE-2026-43093, CVE-2026-43094, CVE-2026-43098, CVE-2026-43099, CVE-2026-43103, CVE-2026-43104, CVE-2026-43105, CVE-2026-43110, CVE-2026-43111, CVE-2026-43112, CVE-2026-43113, CVE-2026-43114, CVE-2026-43116, CVE-2026-43117, CVE-2026-43216, CVE-2026-43219, CVE-2026-43303, CVE-2026-43350, CVE-2026-43421, CVE-2026-43492, CVE-2026-43493, CVE-2026-43494, CVE-2026-43495, CVE-2026-43496, CVE-2026-43497, CVE-2026-43499, CVE-2026-43501, CVE-2026-43502, CVE-2026-45834, CVE-2026-45835, CVE-2026-45836, CVE-2026-45838, CVE-2026-45839, CVE-2026-45840, CVE-2026-45841, CVE-2026-45842, CVE-2026-45843, CVE-2026-45844, CVE-2026-45846, CVE-2026-45850, CVE-2026-45930, CVE-2026-45986, CVE-2026-45987, CVE-2026-45991, CVE-2026-45994, CVE-2026-45996, CVE-2026-45997, CVE-2026-45999, CVE-2026-46002, CVE-2026-46003, CVE-2026-46004, CVE-2026-46005, CVE-2026-46006, CVE-2026-46009, CVE-2026-46015, CVE-2026-46018, CVE-2026-46019, CVE-2026-46021, CVE-2026-46022, CVE-2026-46023, CVE-2026-46024, CVE-2026-46026, CVE-2026-46027, CVE-2026-46031, CVE-2026-46033, CVE-2026-46037, CVE-2026-46038, CVE-2026-46040, CVE-2026-46043, CVE-2026-46044, CVE-2026-46046, CVE-2026-46047, CVE-2026-46049, CVE-2026-46050, CVE-2026-46051, CVE-2026-46052, CVE-2026-46053, CVE-2026-46056, CVE-2026-46058, CVE-2026-46062, CVE-2026-46064, CVE-2026-46065, CVE-2026-46069, CVE-2026-46070, CVE-2026-46072, CVE-2026-46075, CVE-2026-46077, CVE-2026-46078, CVE-2026-46079, CVE-2026-46080, CVE-2026-46082, CVE-2026-46083, CVE-2026-46086, CVE-2026-46088, CVE-2026-46091, CVE-2026-46098, CVE-2026-46099, CVE-2026-46101, CVE-2026-46102, CVE-2026-46103, CVE-2026-46107, CVE-2026-46108, CVE-2026-46109, CVE-2026-46110, CVE-2026-46112, CVE-2026-46113, CVE-2026-46116, CVE-2026-46119, CVE-2026-46120, CVE-2026-46122, CVE-2026-46123, CVE-2026-46124, CVE-2026-46125, CVE-2026-46127, CVE-2026-46128, CVE-2026-46129, CVE-2026-46132, CVE-2026-46133, CVE-2026-46135, CVE-2026-46136, CVE-2026-46137, CVE-2026-46143, CVE-2026-46146, CVE-2026-46149, CVE-2026-46150, CVE-2026-46151, CVE-2026-46159, CVE-2026-46160, CVE-2026-46161, CVE-2026-46163, CVE-2026-46164, CVE-2026-46165, CVE-2026-46167, CVE-2026-46168, CVE-2026-46169, CVE-2026-46172, CVE-2026-46173, CVE-2026-46177, CVE-2026-46178, CVE-2026-46179, CVE-2026-46180, CVE-2026-46184, CVE-2026-46185, CVE-2026-46186, CVE-2026-46187, CVE-2026-46189, CVE-2026-46190, CVE-2026-46191, CVE-2026-46193, CVE-2026-46195, CVE-2026-46196, CVE-2026-46197, CVE-2026-46198, CVE-2026-46199, CVE-2026-46205, CVE-2026-46206, CVE-2026-46208, CVE-2026-46209, CVE-2026-46212, CVE-2026-46214, CVE-2026-46218, CVE-2026-46220, CVE-2026-46227, CVE-2026-46230, CVE-2026-46231, CVE-2026-46233, CVE-2026-46234, CVE-2026-46235, CVE-2026-46236, CVE-2026-46238, CVE-2026-46242, CVE-2026-46273, CVE-2026-46275, CVE-2026-46276, CVE-2026-46280, CVE-2026-46285, CVE-2026-46291, CVE-2026-46292, CVE-2026-46294, CVE-2026-46296, CVE-2026-46299, CVE-2026-46301, CVE-2026-46303, CVE-2026-46304, CVE-2026-46306, CVE-2026-46307, CVE-2026-46314, CVE-2026-46319, CVE-2026-46320, CVE-2026-46321, CVE-2026-46322, CVE-2026-46323, CVE-2026-46331, CVE-2026-52909, CVE-2026-52910, CVE-2026-52911, CVE-2026-52912, CVE-2026-52913, CVE-2026-52914, CVE-2026-52915, CVE-2026-52916, CVE-2026-52917, CVE-2026-52918, CVE-2026-52919, CVE-2026-52920, CVE-2026-52921, CVE-2026-52922, CVE-2026-52923, CVE-2026-52924, CVE-2026-52925, CVE-2026-52926, CVE-2026-52927, CVE-2026-52928, CVE-2026-52929, CVE-2026-52930, CVE-2026-52931, CVE-2026-52933, CVE-2026-52934, CVE-2026-52935, CVE-2026-52939, CVE-2026-52941, CVE-2026-52942, CVE-2026-52943, CVE-2026-52946, CVE-2026-52947, CVE-2026-52948, CVE-2026-52954, CVE-2026-52955, CVE-2026-52957, CVE-2026-52958, CVE-2026-52962, CVE-2026-52963, CVE-2026-52967, CVE-2026-52968, CVE-2026-52969, CVE-2026-52970, CVE-2026-52972, CVE-2026-52974, CVE-2026-52975, CVE-2026-52977, CVE-2026-52981, CVE-2026-52982, CVE-2026-52984, CVE-2026-52985, CVE-2026-52986, CVE-2026-52989, CVE-2026-52992, CVE-2026-52993, CVE-2026-52995, CVE-2026-52998, CVE-2026-52999, CVE-2026-53001, CVE-2026-53002, CVE-2026-53003, CVE-2026-53004, CVE-2026-53006, CVE-2026-53011, CVE-2026-53012, CVE-2026-53016, CVE-2026-53021, CVE-2026-53022, CVE-2026-53023,

CVE-2026-53033, CVE-2026-53034, CVE-2026-53035, CVE-2026-53036, CVE-2026-53037, CVE-2026-53039, CVE-2026-53040, CVE-2026-53041, CVE-2026-53043, CVE-2026-53045, CVE-2026-53046, CVE-2026-53047, CVE-2026-53048, CVE-2026-53049, CVE-2026-53050, CVE-2026-53052, CVE-2026-53056, CVE-2026-53059, CVE-2026-53060, CVE-2026-53061, CVE-2026-53062, CVE-2026-53063, CVE-2026-53064, CVE-2026-53065, CVE-2026-53066, CVE-2026-53068, CVE-2026-53069, CVE-2026-53071, CVE-2026-53072, CVE-2026-53073, CVE-2026-53074, CVE-2026-53075, CVE-2026-53077, CVE-2026-53080, CVE-2026-53082, CVE-2026-53086, CVE-2026-53088, CVE-2026-53093, CVE-2026-53096, CVE-2026-53111, CVE-2026-53112, CVE-2026-53128, CVE-2026-53130, CVE-2026-53131, CVE-2026-53133, CVE-2026-53134, CVE-2026-53135, CVE-2026-53136, CVE-2026-53137, CVE-2026-53138, CVE-2026-53139, CVE-2026-53146, CVE-2026-53147, CVE-2026-53148, CVE-2026-53149, CVE-2026-53150, CVE-2026-53157, CVE-2026-53158, CVE-2026-53159, CVE-2026-53160, CVE-2026-53161, CVE-2026-53163, CVE-2026-53167, CVE-2026-53168, CVE-2026-53176, CVE-2026-53177, CVE-2026-53181, CVE-2026-53182, CVE-2026-53183, CVE-2026-53184, CVE-2026-53186, CVE-2026-53189, CVE-2026-53194, CVE-2026-53195, CVE-2026-53196, CVE-2026-53198, CVE-2026-53199, CVE-2026-53207, CVE-2026-53208, CVE-2026-53209, CVE-2026-53212, CVE-2026-53213, CVE-2026-53215, CVE-2026-53216, CVE-2026-53217, CVE-2026-53218, CVE-2026-53219, CVE-2026-53221, CVE-2026-53223, CVE-2026-53225, CVE-2026-53227, CVE-2026-53228, CVE-2026-53236, CVE-2026-53238, CVE-2026-53239, CVE-2026-53242, CVE-2026-53245, CVE-2026-53249, CVE-2026-53252, CVE-2026-53253, CVE-2026-53254, CVE-2026-53255, CVE-2026-53256, CVE-2026-53263, CVE-2026-53264, CVE-2026-53265, CVE-2026-53266, CVE-2026-53268, CVE-2026-53269, CVE-2026-53270, CVE-2026-53273, CVE-2026-53274, CVE-2026-53275, CVE-2026-53279, CVE-2026-53287, CVE-2026-53289, CVE-2026-53291, CVE-2026-53294, CVE-2026-53295, CVE-2026-53296, CVE-2026-53303, CVE-2026-53304, CVE-2026-53306, CVE-2026-53309, CVE-2026-53314, CVE-2026-53320, CVE-2026-53325, CVE-2026-53329, CVE-2026-53331, CVE-2026-53332, CVE-2026-53337, CVE-2026-53339, CVE-2026-53343, CVE-2026-53349, CVE-2026-53350, CVE-2026-53352, CVE-2026-53354, CVE-2026-53355, CVE-2026-53356, CVE-2026-53359, CVE-2026-53362, CVE-2026-53366, CVE-2026-53392, CVE-2026-53393, CVE-2026-53399, CVE-2026-53400, CVE-2026-53402, CVE-2026-63797, CVE-2026-63806, CVE-2026-63810, CVE-2026-63815, CVE-2026-63818, CVE-2026-63829, CVE-2026-64187, CVE-2026-64189, CVE-2026-64206, CVE-2026-64248, CVE-2026-64250, CVE-2026-64266, CVE-2026-64268, CVE-2026-64269, CVE-2026-64271, CVE-2026-64273, CVE-2026-64274, CVE-2026-64275, CVE-2026-64276, CVE-2026-64277, CVE-2026-64279, CVE-2026-64296, CVE-2026-64297, CVE-2026-64298, CVE-2026-64299, CVE-2026-64301, CVE-2026-64303, CVE-2026-64304, CVE-2026-64306, CVE-2026-64312, CVE-2026-64313, CVE-2026-64315, CVE-2026-64316, CVE-2026-64317, CVE-2026-64318, CVE-2026-64322, CVE-2026-64323, CVE-2026-64324, CVE-2026-64329, CVE-2026-64330, CVE-2026-64331, CVE-2026-64332, CVE-2026-64333, CVE-2026-64334, CVE-2026-64335, CVE-2026-64336, CVE-2026-64337, CVE-2026-64338, CVE-2026-64340, CVE-2026-64342, CVE-2026-64343, CVE-2026-64344, CVE-2026-64346, CVE-2026-64347, CVE-2026-64350, CVE-2026-64351, CVE-2026-64352, CVE-2026-64355, CVE-2026-64359, CVE-2026-64360, CVE-2026-64361, CVE-2026-64362, CVE-2026-64363, CVE-2026-64364, CVE-2026-64365, CVE-2026-64370, CVE-2026-64371, CVE-2026-64372, CVE-2026-64373, CVE-2026-64374, CVE-2026-64375, CVE-2026-64376, CVE-2026-64378, CVE-2026-64379, CVE-2026-64380, CVE-2026-64381, CVE-2026-64390, CVE-2026-64393, CVE-2026-64394, CVE-2026-64395, CVE-2026-64396, CVE-2026-64397, CVE-2026-64398, CVE-2026-64399, CVE-2026-64401, CVE-2026-64403, CVE-2026-64406, CVE-2026-64408, CVE-2026-64409, CVE-2026-64411, CVE-2026-64412, CVE-2026-64413, CVE-2026-64417, CVE-2026-64419, CVE-2026-64420, CVE-2026-64422, CVE-2026-64423, CVE-2026-64425, CVE-2026-64428, CVE-2026-64429, CVE-2026-64430, CVE-2026-64432, CVE-2026-64435, CVE-2026-64436, CVE-2026-64437, CVE-2026-64438, CVE-2026-64440, CVE-2026-64441, CVE-2026-64442, CVE-2026-64443, CVE-2026-64444, CVE-2026-64445, CVE-2026-64446, CVE-2026-64448, CVE-2026-64449, CVE-2026-64450, CVE-2026-64452, CVE-2026-64454, CVE-2026-64455, CVE-2026-64456, CVE-2026-64458, CVE-2026-64461, CVE-2026-64462, CVE-2026-64465, CVE-2026-64468, CVE-2026-64469, CVE-2026-64470, CVE-2026-64471, CVE-2026-64472, CVE-2026-64475, CVE-2026-64476, CVE-2026-64478, CVE-2026-64480, CVE-2026-64482, CVE-2026-64483, CVE-2026-64484, CVE-2026-64486, CVE-2026-64487, CVE-2026-64488, CVE-2026-64489, CVE-2026-64494, CVE-2026-64495, CVE-2026-64496,

CVE-2026-64497, CVE-2026-64500, CVE-2026-64503, CVE-2026-64504, CVE-2026-64505, CVE-2026-64510, CVE-2026-64512, CVE-2026-64514, CVE-2026-64530, CVE-2026-64531, CVE-2026-64532, CVE-2026-64533, CVE-2026-64534, CVE-2026-64535, CVE-2026-64536, CVE-2026-64537, CVE-2026-64538, CVE-2026-64539, CVE-2026-64540, CVE-2026-64541, CVE-2026-64544, CVE-2026-64545, CVE-2026-64546, CVE-2026-64547, CVE-2026-64548, CVE-2026-64549, CVE-2026-64550, CVE-2026-64551, CVE-2026-64552, CVE-2026-64553, CVE-2026-64554, CVE-2026-64557, CVE-2026-64560, CVE-2026-64585, CVE-2026-64593, CVE-2026-64594, CVE-2026-64599, CVE-2026-64600, CVE-2026-64602, CVE-2026-64604) (Bug #59588, Bug #59662, Bug #59713)

- **linux-signed-amd64** (CVE-2023-53292, CVE-2023-53989, CVE-2023-54125, CVE-2023-54271, CVE-2023-54322, CVE-2024-27012, CVE-2024-36013, CVE-2024-36922, CVE-2024-53221, CVE-2024-56657, CVE-2025-10263, CVE-2025-21739, CVE-2025-21863, CVE-2025-22105, CVE-2025-23131, CVE-2025-37864, CVE-2025-38349, CVE-2025-38584, CVE-2025-38627, CVE-2025-38710, CVE-2025-39997, CVE-2025-40196, CVE-2025-40347, CVE-2025-68201, CVE-2025-68315, CVE-2025-68823, CVE-2026-23066, CVE-2026-23255, CVE-2026-23272, CVE-2026-23278, CVE-2026-23302, CVE-2026-23310, CVE-2026-23389, CVE-2026-23399, CVE-2026-23442, CVE-2026-23444, CVE-2026-23468, CVE-2026-31407, CVE-2026-31449, CVE-2026-31488, CVE-2026-31489, CVE-2026-31500, CVE-2026-31532, CVE-2026-31576, CVE-2026-31577, CVE-2026-31578, CVE-2026-31580, CVE-2026-31581, CVE-2026-31583, CVE-2026-31585, CVE-2026-31586, CVE-2026-31587, CVE-2026-31588, CVE-2026-31590, CVE-2026-31594, CVE-2026-31595, CVE-2026-31596, CVE-2026-31597, CVE-2026-31598, CVE-2026-31599, CVE-2026-31602, CVE-2026-31603, CVE-2026-31605, CVE-2026-31607, CVE-2026-31610, CVE-2026-31611, CVE-2026-31612, CVE-2026-31613, CVE-2026-31615, CVE-2026-31616, CVE-2026-31617, CVE-2026-31618, CVE-2026-31619, CVE-2026-31622, CVE-2026-31623, CVE-2026-31624, CVE-2026-31625, CVE-2026-31626, CVE-2026-31627, CVE-2026-31629, CVE-2026-31630, CVE-2026-31637, CVE-2026-31642, CVE-2026-31673, CVE-2026-31676, CVE-2026-31681, CVE-2026-31684, CVE-2026-31685, CVE-2026-31686, CVE-2026-31694, CVE-2026-31696, CVE-2026-31697, CVE-2026-31698, CVE-2026-31699, CVE-2026-31700, CVE-2026-31701, CVE-2026-31702, CVE-2026-31704, CVE-2026-31705, CVE-2026-31708, CVE-2026-31709, CVE-2026-31711, CVE-2026-31712, CVE-2026-31715, CVE-2026-31716, CVE-2026-43052, CVE-2026-43058, CVE-2026-43064, CVE-2026-43071, CVE-2026-43072, CVE-2026-43074, CVE-2026-43075, CVE-2026-43076, CVE-2026-43079, CVE-2026-43080, CVE-2026-43085, CVE-2026-43089, CVE-2026-43093, CVE-2026-43094, CVE-2026-43098, CVE-2026-43099, CVE-2026-43103, CVE-2026-43104, CVE-2026-43105, CVE-2026-43110, CVE-2026-43111, CVE-2026-43112, CVE-2026-43113, CVE-2026-43114, CVE-2026-43116, CVE-2026-43117, CVE-2026-43216, CVE-2026-43219, CVE-2026-43303, CVE-2026-43350, CVE-2026-43421, CVE-2026-43492, CVE-2026-43493, CVE-2026-43494, CVE-2026-43495, CVE-2026-43496, CVE-2026-43497, CVE-2026-43499, CVE-2026-43501, CVE-2026-43502, CVE-2026-45834, CVE-2026-45835, CVE-2026-45836, CVE-2026-45838, CVE-2026-45839, CVE-2026-45840, CVE-2026-45841, CVE-2026-45842, CVE-2026-45843, CVE-2026-45844, CVE-2026-45846, CVE-2026-45850, CVE-2026-45930, CVE-2026-45986, CVE-2026-45987, CVE-2026-45991, CVE-2026-45994, CVE-2026-45996, CVE-2026-45997, CVE-2026-45999, CVE-2026-46002, CVE-2026-46003, CVE-2026-46004, CVE-2026-46005, CVE-2026-46006, CVE-2026-46009, CVE-2026-46015, CVE-2026-46018, CVE-2026-46019, CVE-2026-46021, CVE-2026-46022, CVE-2026-46023, CVE-2026-46024, CVE-2026-46026, CVE-2026-46027, CVE-2026-46031, CVE-2026-46033, CVE-2026-46037, CVE-2026-46038, CVE-2026-46040, CVE-2026-46043, CVE-2026-46044, CVE-2026-46046, CVE-2026-46047, CVE-2026-46049, CVE-2026-46050, CVE-2026-46051, CVE-2026-46052, CVE-2026-46053, CVE-2026-46056, CVE-2026-46058, CVE-2026-46062, CVE-2026-46064, CVE-2026-46065, CVE-2026-46069, CVE-2026-46070, CVE-2026-46072, CVE-2026-46075, CVE-2026-46077, CVE-2026-46078, CVE-2026-46079, CVE-2026-46080, CVE-2026-46082, CVE-2026-46083, CVE-2026-46086, CVE-2026-46088, CVE-2026-46091, CVE-2026-46098, CVE-2026-46099, CVE-2026-46101, CVE-2026-46102, CVE-2026-46103, CVE-2026-46107, CVE-2026-46108, CVE-2026-46109, CVE-2026-46110, CVE-2026-46112, CVE-2026-46113, CVE-2026-46116, CVE-2026-46119, CVE-2026-46120, CVE-2026-46122, CVE-2026-46123, CVE-2026-46124, CVE-2026-46125, CVE-2026-46127, CVE-2026-46128, CVE-2026-46129, CVE-2026-46132, CVE-2026-46133, CVE-2026-46135, CVE-2026-46136, CVE-2026-46137, CVE-2026-46143, CVE-2026-46146, CVE-2026-46149, CVE-2026-46150, CVE-2026-46151, CVE-2026-46159,

CVE-2026-46160, CVE-2026-46161, CVE-2026-46163, CVE-2026-46164, CVE-2026-46165, CVE-2026-46167, CVE-2026-46168, CVE-2026-46169, CVE-2026-46172, CVE-2026-46173, CVE-2026-46177, CVE-2026-46178, CVE-2026-46179, CVE-2026-46180, CVE-2026-46184, CVE-2026-46185, CVE-2026-46186, CVE-2026-46187, CVE-2026-46189, CVE-2026-46190, CVE-2026-46191, CVE-2026-46193, CVE-2026-46195, CVE-2026-46196, CVE-2026-46197, CVE-2026-46198, CVE-2026-46199, CVE-2026-46205, CVE-2026-46206, CVE-2026-46208, CVE-2026-46209, CVE-2026-46212, CVE-2026-46214, CVE-2026-46218, CVE-2026-46220, CVE-2026-46227, CVE-2026-46230, CVE-2026-46231, CVE-2026-46233, CVE-2026-46234, CVE-2026-46235, CVE-2026-46236, CVE-2026-46238, CVE-2026-46242, CVE-2026-46273, CVE-2026-46275, CVE-2026-46276, CVE-2026-46280, CVE-2026-46285, CVE-2026-46291, CVE-2026-46292, CVE-2026-46294, CVE-2026-46296, CVE-2026-46299, CVE-2026-46301, CVE-2026-46303, CVE-2026-46304, CVE-2026-46306, CVE-2026-46307, CVE-2026-46314, CVE-2026-46319, CVE-2026-46320, CVE-2026-46321, CVE-2026-46322, CVE-2026-46323, CVE-2026-46331, CVE-2026-52909, CVE-2026-52910, CVE-2026-52911, CVE-2026-52912, CVE-2026-52913, CVE-2026-52914, CVE-2026-52915, CVE-2026-52916, CVE-2026-52917, CVE-2026-52918, CVE-2026-52919, CVE-2026-52920, CVE-2026-52921, CVE-2026-52922, CVE-2026-52923, CVE-2026-52924, CVE-2026-52925, CVE-2026-52926, CVE-2026-52927, CVE-2026-52928, CVE-2026-52929, CVE-2026-52930, CVE-2026-52931, CVE-2026-52933, CVE-2026-52934, CVE-2026-52935, CVE-2026-52939, CVE-2026-52941, CVE-2026-52942, CVE-2026-52943, CVE-2026-52946, CVE-2026-52947, CVE-2026-52948, CVE-2026-52954, CVE-2026-52955, CVE-2026-52957, CVE-2026-52958, CVE-2026-52962, CVE-2026-52963, CVE-2026-52967, CVE-2026-52968, CVE-2026-52969, CVE-2026-52970, CVE-2026-52972, CVE-2026-52974, CVE-2026-52975, CVE-2026-52977, CVE-2026-52981, CVE-2026-52982, CVE-2026-52984, CVE-2026-52985, CVE-2026-52986, CVE-2026-52989, CVE-2026-52992, CVE-2026-52993, CVE-2026-52995, CVE-2026-52998, CVE-2026-52999, CVE-2026-53001, CVE-2026-53002, CVE-2026-53003, CVE-2026-53004, CVE-2026-53006, CVE-2026-53011, CVE-2026-53012, CVE-2026-53016, CVE-2026-53021, CVE-2026-53022, CVE-2026-53023, CVE-2026-53033, CVE-2026-53034, CVE-2026-53035, CVE-2026-53036, CVE-2026-53037, CVE-2026-53039, CVE-2026-53040, CVE-2026-53041, CVE-2026-53043, CVE-2026-53045, CVE-2026-53046, CVE-2026-53047, CVE-2026-53048, CVE-2026-53049, CVE-2026-53050, CVE-2026-53052, CVE-2026-53056, CVE-2026-53059, CVE-2026-53060, CVE-2026-53061, CVE-2026-53062, CVE-2026-53063, CVE-2026-53064, CVE-2026-53065, CVE-2026-53066, CVE-2026-53068, CVE-2026-53069, CVE-2026-53071, CVE-2026-53072, CVE-2026-53073, CVE-2026-53074, CVE-2026-53075, CVE-2026-53077, CVE-2026-53080, CVE-2026-53082, CVE-2026-53086, CVE-2026-53088, CVE-2026-53093, CVE-2026-53096, CVE-2026-53111, CVE-2026-53112, CVE-2026-53128, CVE-2026-53130, CVE-2026-53131, CVE-2026-53133, CVE-2026-53134, CVE-2026-53135, CVE-2026-53136, CVE-2026-53137, CVE-2026-53138, CVE-2026-53139, CVE-2026-53146, CVE-2026-53147, CVE-2026-53148, CVE-2026-53149, CVE-2026-53150, CVE-2026-53157, CVE-2026-53158, CVE-2026-53159, CVE-2026-53160, CVE-2026-53161, CVE-2026-53163, CVE-2026-53167, CVE-2026-53168, CVE-2026-53176, CVE-2026-53177, CVE-2026-53181, CVE-2026-53182, CVE-2026-53183, CVE-2026-53184, CVE-2026-53186, CVE-2026-53189, CVE-2026-53194, CVE-2026-53195, CVE-2026-53196, CVE-2026-53198, CVE-2026-53199, CVE-2026-53207, CVE-2026-53208, CVE-2026-53209, CVE-2026-53212, CVE-2026-53213, CVE-2026-53215, CVE-2026-53216, CVE-2026-53217, CVE-2026-53218, CVE-2026-53219, CVE-2026-53221, CVE-2026-53223, CVE-2026-53225, CVE-2026-53227, CVE-2026-53228, CVE-2026-53236, CVE-2026-53238, CVE-2026-53239, CVE-2026-53242, CVE-2026-53245, CVE-2026-53249, CVE-2026-53252, CVE-2026-53253, CVE-2026-53254, CVE-2026-53255, CVE-2026-53256, CVE-2026-53263, CVE-2026-53264, CVE-2026-53265, CVE-2026-53266, CVE-2026-53268, CVE-2026-53269, CVE-2026-53270, CVE-2026-53273, CVE-2026-53274, CVE-2026-53275, CVE-2026-53279, CVE-2026-53287, CVE-2026-53289, CVE-2026-53291, CVE-2026-53294, CVE-2026-53295, CVE-2026-53296, CVE-2026-53303, CVE-2026-53304, CVE-2026-53306, CVE-2026-53309, CVE-2026-53314, CVE-2026-53320, CVE-2026-53325, CVE-2026-53329, CVE-2026-53331, CVE-2026-53332, CVE-2026-53337, CVE-2026-53339, CVE-2026-53343, CVE-2026-53349, CVE-2026-53350, CVE-2026-53352, CVE-2026-53354, CVE-2026-53355, CVE-2026-53356, CVE-2026-53359, CVE-2026-53362, CVE-2026-53366, CVE-2026-53392, CVE-2026-53393, CVE-2026-53399, CVE-2026-53400, CVE-2026-53402, CVE-2026-63797, CVE-2026-63810, CVE-2026-63815, CVE-2026-63818, CVE-2026-63829, CVE-2026-64187, CVE-2026-64189, CVE-2026-64206,

CVE-2026-64266, CVE-2026-64268, CVE-2026-64269, CVE-2026-64271, CVE-2026-64273, CVE-2026-64274, CVE-2026-64275, CVE-2026-64276, CVE-2026-64277, CVE-2026-64279, CVE-2026-64296, CVE-2026-64297, CVE-2026-64298, CVE-2026-64299, CVE-2026-64301, CVE-2026-64303, CVE-2026-64304, CVE-2026-64306, CVE-2026-64312, CVE-2026-64313, CVE-2026-64315, CVE-2026-64316, CVE-2026-64317, CVE-2026-64318, CVE-2026-64322, CVE-2026-64323, CVE-2026-64324, CVE-2026-64329, CVE-2026-64330, CVE-2026-64331, CVE-2026-64332, CVE-2026-64333, CVE-2026-64334, CVE-2026-64335, CVE-2026-64336, CVE-2026-64337, CVE-2026-64338, CVE-2026-64340, CVE-2026-64342, CVE-2026-64343, CVE-2026-64344, CVE-2026-64346, CVE-2026-64347, CVE-2026-64350, CVE-2026-64351, CVE-2026-64352, CVE-2026-64355, CVE-2026-64359, CVE-2026-64360, CVE-2026-64361, CVE-2026-64362, CVE-2026-64363, CVE-2026-64364, CVE-2026-64365, CVE-2026-64372, CVE-2026-64373, CVE-2026-64374, CVE-2026-64376, CVE-2026-64379, CVE-2026-64380, CVE-2026-64381, CVE-2026-64390, CVE-2026-64393, CVE-2026-64394, CVE-2026-64395, CVE-2026-64396, CVE-2026-64397, CVE-2026-64398, CVE-2026-64399, CVE-2026-64401, CVE-2026-64403, CVE-2026-64406, CVE-2026-64408, CVE-2026-64409, CVE-2026-64411, CVE-2026-64412, CVE-2026-64413, CVE-2026-64417, CVE-2026-64419, CVE-2026-64422, CVE-2026-64423, CVE-2026-64425, CVE-2026-64428, CVE-2026-64429, CVE-2026-64436, CVE-2026-64437, CVE-2026-64438, CVE-2026-64440, CVE-2026-64445, CVE-2026-64446, CVE-2026-64449, CVE-2026-64450, CVE-2026-64452, CVE-2026-64454, CVE-2026-64455, CVE-2026-64456, CVE-2026-64458, CVE-2026-64461, CVE-2026-64462, CVE-2026-64465, CVE-2026-64468, CVE-2026-64469, CVE-2026-64470, CVE-2026-64471, CVE-2026-64472, CVE-2026-64476, CVE-2026-64478, CVE-2026-64483, CVE-2026-64487, CVE-2026-64494, CVE-2026-64495, CVE-2026-64496, CVE-2026-64497, CVE-2026-64500, CVE-2026-64504, CVE-2026-64505, CVE-2026-64512, CVE-2026-64514, CVE-2026-64530, CVE-2026-64531, CVE-2026-64534, CVE-2026-64535, CVE-2026-64537, CVE-2026-64538, CVE-2026-64539, CVE-2026-64540, CVE-2026-64544, CVE-2026-64545, CVE-2026-64546, CVE-2026-64547, CVE-2026-64549, CVE-2026-64550, CVE-2026-64551, CVE-2026-64552, CVE-2026-64553, CVE-2026-64554, CVE-2026-64557, CVE-2026-64560, CVE-2026-64600) (Bug #59588, Bug #59662, Bug #59713)

- **mariadb** (CVE-2025-13699, CVE-2026-21968, CVE-2026-34303, CVE-2026-3494, CVE-2026-44168, CVE-2026-44170, CVE-2026-44171, CVE-2026-44172, CVE-2026-44173, CVE-2026-48163, CVE-2026-48165, CVE-2026-49261) (Bug #59613)
- **mesa** (CVE-2026-40393) (Bug #59609)
- **nss** (CVE-2026-12318, CVE-2026-16389, CVE-2026-6766, CVE-2026-6767, CVE-2026-6772) (Bug #59688, Bug #59748)
- **nvidia-graphics-drivers** (CVE-2025-23280, CVE-2025-23282, CVE-2025-23300, CVE-2025-23330, CVE-2025-23332, CVE-2025-23345, CVE-2025-33219) (Bug #59775)
- **openjdk-17** (CVE-2026-22007, CVE-2026-22013, CVE-2026-22016, CVE-2026-22018, CVE-2026-22021, CVE-2026-23865, CVE-2026-34268, CVE-2026-34282, CVE-2026-41254, CVE-2026-46917, CVE-2026-46968, CVE-2026-47010, CVE-2026-47021, CVE-2026-47027, CVE-2026-47059, CVE-2026-47063, CVE-2026-60147, CVE-2026-60589, CVE-2026-61308, CVE-2026-70907) (Bug #59699, Bug #59858)
- **openssl** (CVE-2026-34180, CVE-2026-34182, CVE-2026-42766, CVE-2026-42770, CVE-2026-45445, CVE-2026-45446, CVE-2026-45447, CVE-2026-7383, CVE-2026-9076) (Bug #59497)
- **pam** (CVE-2024-22365, CVE-2025-6020) (Bug #58946)
- **pcre2** (CVE-2026-86145) (Bug #59909)
- **poppler** (CVE-2024-6239, CVE-2025-43718, CVE-2025-43903, CVE-2025-50420, CVE-2025-52885, CVE-2025-52886, CVE-2026-10118) (Bug #59499, Bug #59698)
- **postgresql-15** (CVE-2025-8714, CVE-2026-14662, CVE-2026-14663, CVE-2026-14664, CVE-2026-14666, CVE-2026-14668, CVE-2026-14669, CVE-2026-14670, CVE-2026-14671, CVE-2026-14672, CVE-2026-14673, CVE-2026-14676, CVE-2026-14677, CVE-2026-14678, CVE-2026-14679, CVE-2026-14680, CVE-2026-14681, CVE-2026-15741, CVE-2026-15742,

CVE-2026-16238, CVE-2026-16239, CVE-2026-16241, CVE-2026-18024, CVE-2026-18408, CVE-2026-19385, CVE-2026-6464, CVE-2026-6469, CVE-2026-6470, CVE-2026-6471, CVE-2026-6473) (Bug #59751)

- **protobuf** (CVE-2024-7254, CVE-2025-4565, CVE-2026-0994, CVE-2026-6409) (Bug #59620)
- **pydantic** (CVE-2024-3772) (Bug #59614)
- **python-httplib2** (CVE-2026-59939) (Bug #59774)
- **python-markdown** (CVE-2025-69534) (Bug #59623)
- **python-urllib3** (CVE-2026-44431) (Bug #59571)
- **python3.11** (CVE-2023-52425, CVE-2025-13462, CVE-2026-0672, CVE-2026-2297, CVE-2026-3644, CVE-2026-4224, CVE-2026-4519, CVE-2026-6100) (Bug #59628)
- **rsync** (CVE-2026-45232) (Bug #59624)
- **samba** (CVE-2026-58216, CVE-2026-58218, CVE-2026-58221, CVE-2026-58222, CVE-2026-58224, CVE-2026-6949) (Bug #59665)
- **shim** (CVE-2024-2312) (Bug #59616)
- **shim-helpers-amd64-signed** (CVE-2024-2312) (Bug #59616)
- **shim-signed** (CVE-2024-2312) (Bug #59616)
- **squid** (CVE-2026-33515, CVE-2026-33526, CVE-2026-47729, CVE-2026-50012) (Bug #59682)
- **univention-directory-manager-rest** (Bug #59761)
- **xorg-server** (CVE-2022-49737, CVE-2026-50256, CVE-2026-50257, CVE-2026-50258, CVE-2026-50259, CVE-2026-50260, CVE-2026-50261, CVE-2026-50262, CVE-2026-50263, CVE-2026-50264) (Bug #59750)
- **xz-utils** (CVE-2026-34743) (Bug #59619)

- Univention Corporate Server 5.2-7 includes the following updated packages from Debian 12.15:
  - **appstream**
  - **beets**
  - **ca-certificates**
  - **dcmtk**
  - **debian-installer**
  - **ghdl**
  - **gss**
  - **indi-orion-ssg3**
  - **jackson-core**
  - **kernel-wedge**
  - **libapache-session-browseable-perl**
  - **libass**
  - **libcaca**
  - **libdbd-csv-perl**
  - **libgd-perl**
  - **libhtml-gumbo-perl**
  - **libmatio**
  - **libtext-csv-xs-perl**

- **linux-base**
- **linuxcnc**
- **llvm-toolchain-22**
- **mistral**
- **node-regexpp**
- **nvidia-settings**
- **ojalgo**
- **okular**
- **openslide**
- **phpunit**
- **rlottie**
- **ruby-css-parser**
- **sentry-python**
- **sslh**
- **swift**
- **sylpheed**
- **sympa**
- **u-boot**
- **wolfssl**

CHAPTER

TWO

BASIC SYSTEM SERVICES

2.1 Univention Configuration Registry

- The C library of UCR now supports arbitrary variable value lengths instead of cutting the values at 1024 chars (Bug #51864).

2.2 Other system services

- `univention-ssh` now deactivates SSH public key authentication when authenticating with machine account credentials. This avoids authentication failures caused by excessive SSH authentication attempts. Further security-related configuration options for joined systems have been added (Bug #59144).

CHAPTER

THREE

DOMAIN SERVICES

- The `server_password_change` utilities no longer print `Bad file descriptor` error messages when invoked through Debian post-installation scripts. In this case, the utilities write debug output to standard error instead (Bug #56630).
- Database connection and authentication failures no longer produce repeated Python tracebacks during system installation. The failures are now logged as concise error messages (Bug #51671).

3.1 OpenLDAP

- The configuration of the OpenLDAP `memberof` overlay moved into the `univention-ldap-server` package. The `univention-ldap-overlay-memberof` package is now an empty transitional package. You can safely remove it (Bug #47464).
- The LDAP server could crash during a simple bind when an account using the `{KINIT}` password scheme had no `krb5PrincipalName` attribute or when a Kerberos lookup failed. Repeated bind attempts could also leak memory, and temporary password data was not always completely cleared. The LDAP overlay module now handles these cases safely, releases Kerberos resources correctly, and clears the complete temporary password buffer (Bug #59920).
- The LDAP server could crash during concurrent simple binds using the `{KINIT}` password scheme because authentication requests shared Kerberos state. Each bind now uses an isolated Kerberos context, preventing memory corruption and ensuring that authentication resources are released safely (Bug #59921).
- Disabling a user account no longer invalidates the password hash stored in the LDAP attribute `userPassword`. This allows the Keycloak Identity Provider to distinguish a disabled account from invalid credentials and report the appropriate authentication error. The `shadowbind` LDAP overlay is now mandatory to ensure that disabled user accounts cannot authenticate using LDAP bind (Bug #59898).

3.1.1 Listener/Notifier domain replication

- The directory replication OID skip list now contains the built-in schema definitions from OpenLDAP 2.6 to allow mixed environments with UCS 5.3 (Bug #59532).
- The Univention Directory Listener shutdown handling is now signal-safe to avoid segmentation faults when terminating while embedded Python handler code is active (Bug #59541).

3.2 LDAP Directory Manager

- Paginated searches returned an empty result when requesting a page number that isn't larger than the previously requested one, for example when navigating back to a previous page (Bug #59466).
- The performance of object searches using `opened=0` has been improved. The API now avoids loading and decoding full UDM objects when it only requests object metadata. This significantly speeds up large search result sets (Bug #59579).
- The UDM module search API has been extended to allow passing `opened=True` for UDM modules which support it (Bug #59579).

- Total user-count metrics now exclude system accounts (Bug #59634).
- The `opened` query parameter of the object search was missing from the OpenAPI/Swagger schema and is now included (Bug #59575).
- The UDM HTTP REST API command line doesn't depend on the UCR default layer anymore for compatibility with Nubus for Kubernetes (Bug #59837).
- The experimental delegative administration feature can cause UDM functionality to crash when it processes invalid LDAP data. UDM now ignores affected properties during delegative administration evaluation (Bug #59560).
- The performance of object processing has been improved by reducing the overhead of mapping LDAP attributes to UDM properties. In environments with many objects, such as when retrieving large result sets through the UDM HTTP REST API, this noticeably speeds up object retrieval (Bug #59578).
- The syntax validation for Guardian role values has been relaxed. Role identifiers are no longer restricted to the previous `app:namespace:role` format, allowing arbitrary role strings to be used (Bug #59603).
- The generation of the `sambaNTPassword` LDAP attribute can now be deactivated through the UCR variable `password/samba/nthash`. When deactivated, existing NT hashes are removed during the next password change. Be aware that this breaks services relying on NT password hashes, including S4/AD Connector password synchronization, Squid NTLM authentication, and RADIUS MS-CHAP/NTLM authentication (Bug #59607).
- The `--list-dns` option of `univention-license-check` was broken by erratum 394 and has been repaired (Bug #59633).
- The order of extended attributes in the layout has been corrected in cases where no built-in layout elements exist for a custom tab. UDM now displays custom groups and properties in a consistent and predictable order (Bug #48612).
- The default authorization role `udm:default-roles:helpdesk-operator` for the experimental delegative administration feature was missing read permissions for mandatory user properties (`username`, `lastname`, `primaryGroup`, `unixhome`, `mailForwardCopyToSelf`). This caused errors when opening or saving user objects in UMC as a helpdesk operator (Bug #59673).

CHAPTER

FOUR

UNIVENTION MANAGEMENT CONSOLE

4.1 Univention Management Console web interface

- When users deselect a single item from an all-selected state, the grid header *select all* checkbox now displays the unselected state instead of the indeterminate state (Bug #59147).
- The DOMpurify library has been upgraded to the latest version (2.5.9, Bug #59808).

4.2 Univention App Center

- The App Center has been adapted to be compatible with future `ruamel.yaml` API deprecations (Bug #59521).
- The App Center UMC module is now able to handle the installation of new dependencies during the upgrade of an app (Bug #59717).
- Apps that can be installed multiple times in the domain can now specify whether to install first on the *Primary Directory Node* (Bug #59895).
- An internal flag for `univention-app register listener` has been added. This allows the forced removal of a listener module and the listener-trigger service (Bug #59919).

4.3 Modules for system settings / setup wizard

- The system setup no longer selects the `univention-ldap-overlay-memberof` package for installation, as the OpenLDAP `memberof` overlay configuration is now part of the `univention-ldap-server` package (Bug #47464).
- Automatic DNS updates of the SSO record during IP address changes now correctly honor the UCR variable `keycloak/server/sso/autoregistration` (Bug #59759).
- The IP address registration during system startup no longer incorrectly reports a host's existing IP address as already in use (Bug #53252, Bug #59759).

4.4 User management

- The Self Service now uses clearer wording for the email address used for account recovery (Bug #59583).

4.5 System diagnostic module

- The error message for the `11_nameserver` check was broken and has been corrected (Bug #59489).
- The `20_check_share_references` check now only runs on the *Primary Directory Node*. It binds as the machine account, which on a UCS@school school replica may not read the objects of other schools, so shares referencing a server of another school were incorrectly reported as dangling references (Bug #59718).

4.6 LDAP directory browser

- Set `*` as default search value when automatic substring search is deactivated (Bug #59444).
- The performance of object searches using `opened=0` has been improved. The API now avoids loading and decoding full UDM objects when it only requests object metadata. This significantly speeds up large search result sets (Bug #59579).
- The experimental paginated object search supports LDAP Server Side Sorting (SSS) with either Simple Paged Results (SPR) or Virtual List View (VLV). Use this feature for evaluation only. Univention doesn't support it for production use yet. Known limitations affect scalability, process-local pagination state, and recovery after LDAP server restarts. To use VLV, enable the LDAP SSSVLV overlay and configure it correctly (Bug #50240).
- Empty search queries now always return all results (Bug #59595).

CHAPTER

FIVE

UNIVENTION BASE LIBRARIES

- You can configure the timeout for LDAP extension activation in `ucs_registerLDAPExtension` through the UCR variable `directory/manager/ldap_extension/timeout/activation` (Bug #59474).
- Authentication retry handling in the UMC client has been corrected. Previously, under certain authentication failures, the client could repeatedly retry authentication until it reached the Python recursion limit. The retry logic now performs a limited number of authentication attempts before reporting the authentication failure to the caller (Bug #58380).

CHAPTER

SIX

SYSTEM SERVICES

6.1 SAML

- The SAML integration now supports API changes in newer `python-keycloak` versions (Bug #59517).
- The **`crudesaml`** package epoch has been increased to ensure a valid upgrade path to UCS 5.3 and restore the original upstream package version (Bug #59511).

6.2 Mail services

6.2.1 IMAP services

- UCS 5.3 upgrades with Dovecot 2.4 now use the UCR template `/etc/dovecot/conf.d/90-sieve-extprograms.conf` to write a compatible configuration file (Bug #59520).

6.3 RADIUS

- The username of the inner tunnel is now passed to the default connection. For example, this allows assigning a VLAN based on this authenticated username instead of inheriting unverified settings from the outer tunnel ("anonymous login", Bug #59456).
- The performance of NTLM authentication with RADIUS has been significantly improved, reducing authentication times and CPU load under high request volumes. The `univention-radius-ntlm-auth` helper has been rewritten in Rust for this purpose (Bug #59042).

6.4 PAM / Local group cache

- Printing with iPads could cause CUPS to hang or slow down the print dialog. The `pam_krb5` Kerberos authentication step is now skipped in the PAM auth stack when the service is `cups`, preventing unnecessary Kerberos lookups during CUPS authentication (Bug #59552).

6.5 Networking services

- During system startup, IP address registration now retries temporary communication failures while Univention Management Console services are still starting instead of failing (Bug #53252).

CHAPTER

SEVEN

SERVICES FOR WINDOWS

7.1 Samba

- Windows domain trust validation could fail because `winbindd` got stuck attempting an SMB connection that Microsoft Active Directory neither required nor permitted. For example, this occurred when Active Directory enabled `Require NTLMv2 session security` (Bug #59601).
- Samba 4.24 now lets Windows clients open symbolic links (Bug #59706).

7.2 Univention S4 Connector

- The S4 Connector now retries primary group synchronization after the corresponding group becomes available in Samba/AD (Bug #52788).

7.3 Univention Active Directory Connection

- During password synchronization to UCS, the `univention-ad-connector` now sets the `msDS-SupportedEncryptionTypes` attribute in Active Directory only for bidirectional synchronization configurations (Bug #59692).
- The AD Connector now retries primary group synchronization after the corresponding group becomes available in AD (Bug #59694).
- The `allowfilter` and `ignorefilter` settings from the AD Connector now support basic substring matching for values, for example `*string*` (Bug #59701).
- During password synchronization from Active Directory to UCS, the AD Connector now synchronizes Kerberos keys by default. This lets UCS use more secure key types after a password change in Active Directory (Bug #57689).

CHAPTER

EIGHT

OTHER CHANGES

- The Python LDAP client now correctly preserves the LDAP Virtual List View (VLV) search context between requests. This significantly improves the performance of repeated VLV requests and reduces server load when applications use VLV-based pagination, such as the experimental pagination feature of the UDM HTTP REST API (Bug #59666).
- The Cerbos Python SDK provides Python clients for accessing Cerbos. In UCS, it supports HTTP only, not gRPC (Bug #59901).
- This is the first release of the Cerbos-based Guardian component for UCS. It replaces the OPA-based Guardian and is intended for use only with Univention software. There is no upgrade path from the OPA-based Guardian to the new component. This update removes the OPA-based Guardian, so you don't need to take any action (Bug #59669).

INDEX

B

C

CVE

D

E

K

P