



Changelog for Univention Corporate Server (UCS) 5.2-1

Release 5.2-1

Mar 11, 2025

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

CONTENTS

1	General	1
2	Univention Management Console	5
2.1	User management	5
3	Software deployment	7
4	System services	9
4.1	SAML	9
4.2	Proxy services	9
	Index	11

GENERAL

- Univention Corporate Server 5.2-1 includes all security updates issued for UCS 5.2-0:
 - **avahi** (CVE-2023-38469, CVE-2023-38470, CVE-2023-38471, CVE-2023-38472, CVE-2023-38473) (Bug #57914)
 - **bind9** (CVE-2024-11187, CVE-2024-12705) (Bug #57926)
 - **firefox-esr** (CVE-2024-11704, CVE-2025-0237, CVE-2025-0238, CVE-2025-0239, CVE-2025-0240, CVE-2025-0241, CVE-2025-0242, CVE-2025-0243, CVE-2025-1009, CVE-2025-1010, CVE-2025-1011, CVE-2025-1012, CVE-2025-1013, CVE-2025-1014, CVE-2025-1016, CVE-2025-1017) (Bug #57919, Bug #57950)
 - **git** (CVE-2024-50349, CVE-2024-52006) (Bug #57911)
 - **glib2.0** (CVE-2024-52533) (Bug #57920)
 - **gnutls28** (CVE-2024-12133, CVE-2024-12243) (Bug #57969)
 - **gsl** (CVE-2020-35357) (Bug #57923)
 - **intel-microcode** (CVE-2024-21820, CVE-2024-21853, CVE-2024-23918) (Bug #57916)
 - **jinja2** (CVE-2024-22195, CVE-2024-34064) (Bug #57927)
 - **libsoup2.4** (CVE-2024-52530, CVE-2024-52531, CVE-2024-52532) (Bug #57924)
 - **libtasn1-6** (CVE-2024-12133) (Bug #57966)
 - **linux** (CVE-2022-49034, CVE-2023-52916, CVE-2024-26595, CVE-2024-27407, CVE-2024-35870, CVE-2024-35956, CVE-2024-36479, CVE-2024-36899, CVE-2024-37021, CVE-2024-41014, CVE-2024-42252, CVE-2024-42315, CVE-2024-42319, CVE-2024-43098, CVE-2024-44950, CVE-2024-45828, CVE-2024-46809, CVE-2024-46841, CVE-2024-46896, CVE-2024-47143, CVE-2024-47408, CVE-2024-47745, CVE-2024-48881, CVE-2024-49571, CVE-2024-49861, CVE-2024-49891, CVE-2024-49897, CVE-2024-49898, CVE-2024-49899, CVE-2024-49909, CVE-2024-49911, CVE-2024-49915, CVE-2024-49917, CVE-2024-49925, CVE-2024-49929, CVE-2024-49934, CVE-2024-49939, CVE-2024-49951, CVE-2024-49994, CVE-2024-49996, CVE-2024-50014, CVE-2024-50047, CVE-2024-50051, CVE-2024-50055, CVE-2024-50121, CVE-2024-50146, CVE-2024-50164, CVE-2024-50248, CVE-2024-50258, CVE-2024-50275, CVE-2024-50304, CVE-2024-52332, CVE-2024-53099, CVE-2024-53105, CVE-2024-53124, CVE-2024-53125, CVE-2024-53128, CVE-2024-53141, CVE-2024-53142, CVE-2024-53145, CVE-2024-53146, CVE-2024-53148, CVE-2024-53150, CVE-2024-53151, CVE-2024-53154, CVE-2024-53155, CVE-2024-53156, CVE-2024-53157, CVE-2024-53158, CVE-2024-53161, CVE-2024-53164, CVE-2024-53165, CVE-2024-53170, CVE-2024-53171, CVE-2024-53172, CVE-2024-53173, CVE-2024-53174, CVE-2024-53175, CVE-2024-53180, CVE-2024-53181, CVE-2024-53183, CVE-2024-53184, CVE-2024-53190, CVE-2024-53194, CVE-2024-53196, CVE-2024-53197, CVE-2024-53198, CVE-2024-53206, CVE-2024-53207, CVE-2024-53208, CVE-2024-53210, CVE-2024-53213, CVE-2024-53214, CVE-2024-53215, CVE-2024-53217, CVE-2024-53220, CVE-2024-53226, CVE-2024-53227, CVE-2024-53229, CVE-2024-53230, CVE-2024-53231, CVE-2024-53233, CVE-2024-53237, CVE-2024-53239, CVE-2024-53240, CVE-2024-53241, CVE-2024-53680, CVE-2024-53685, CVE-2024-53690, CVE-2024-55881, CVE-2024-55916, CVE-2024-56369, CVE-2024-56531, CVE-2024-56532)

- CVE-2024-56533, CVE-2024-56539, CVE-2024-56546, CVE-2024-56548, CVE-2024-56551,
CVE-2024-56557, CVE-2024-56558, CVE-2024-56562, CVE-2024-56567, CVE-2024-56568,
CVE-2024-56569, CVE-2024-56570, CVE-2024-56571, CVE-2024-56572, CVE-2024-56574,
CVE-2024-56575, CVE-2024-56576, CVE-2024-56578, CVE-2024-56579, CVE-2024-56581,
CVE-2024-56582, CVE-2024-56584, CVE-2024-56585, CVE-2024-56586, CVE-2024-56587,
CVE-2024-56589, CVE-2024-56590, CVE-2024-56593, CVE-2024-56594, CVE-2024-56595,
CVE-2024-56596, CVE-2024-56597, CVE-2024-56598, CVE-2024-56599, CVE-2024-56600,
CVE-2024-56601, CVE-2024-56602, CVE-2024-56603, CVE-2024-56604, CVE-2024-56605,
CVE-2024-56606, CVE-2024-56608, CVE-2024-56610, CVE-2024-56614, CVE-2024-56615,
CVE-2024-56616, CVE-2024-56619, CVE-2024-56622, CVE-2024-56623, CVE-2024-56625,
CVE-2024-56626, CVE-2024-56627, CVE-2024-56628, CVE-2024-56629, CVE-2024-56630,
CVE-2024-56631, CVE-2024-56633, CVE-2024-56634, CVE-2024-56636, CVE-2024-56637,
CVE-2024-56640, CVE-2024-56642, CVE-2024-56643, CVE-2024-56644, CVE-2024-56645,
CVE-2024-56648, CVE-2024-56650, CVE-2024-56651, CVE-2024-56658, CVE-2024-56659,
CVE-2024-56660, CVE-2024-56661, CVE-2024-56662, CVE-2024-56663, CVE-2024-56664,
CVE-2024-56665, CVE-2024-56670, CVE-2024-56672, CVE-2024-56675, CVE-2024-56677,
CVE-2024-56678, CVE-2024-56679, CVE-2024-56681, CVE-2024-56683, CVE-2024-56687,
CVE-2024-56688, CVE-2024-56690, CVE-2024-56691, CVE-2024-56693, CVE-2024-56694,
CVE-2024-56698, CVE-2024-56700, CVE-2024-56701, CVE-2024-56703, CVE-2024-56704,
CVE-2024-56705, CVE-2024-56707, CVE-2024-56708, CVE-2024-56709, CVE-2024-56715,
CVE-2024-56716, CVE-2024-56717, CVE-2024-56718, CVE-2024-56720, CVE-2024-56722,
CVE-2024-56723, CVE-2024-56724, CVE-2024-56725, CVE-2024-56726, CVE-2024-56727,
CVE-2024-56728, CVE-2024-56739, CVE-2024-56741, CVE-2024-56745, CVE-2024-56746,
CVE-2024-56747, CVE-2024-56748, CVE-2024-56751, CVE-2024-56754, CVE-2024-56755,
CVE-2024-56756, CVE-2024-56759, CVE-2024-56763, CVE-2024-56765, CVE-2024-56766,
CVE-2024-56767, CVE-2024-56769, CVE-2024-56770, CVE-2024-56774, CVE-2024-56776,
CVE-2024-56777, CVE-2024-56778, CVE-2024-56779, CVE-2024-56780, CVE-2024-56781,
CVE-2024-56783, CVE-2024-56785, CVE-2024-56787, CVE-2024-57791, CVE-2024-57792,
CVE-2024-57798, CVE-2024-57807, CVE-2024-57838, CVE-2024-57849, CVE-2024-57850,
CVE-2024-57874, CVE-2024-57876, CVE-2024-57887, CVE-2024-57892, CVE-2024-57907,
CVE-2024-57946) (Bug #57913, Bug #57948)
- **linux-signed-amd64** (CVE-2023-52916, CVE-2024-27407, CVE-2024-35870,
CVE-2024-35956, CVE-2024-36479, CVE-2024-36899, CVE-2024-37021, CVE-2024-41014,
CVE-2024-42252, CVE-2024-42315, CVE-2024-44950, CVE-2024-46809, CVE-2024-49861,
CVE-2024-49891, CVE-2024-49897, CVE-2024-49898, CVE-2024-49899, CVE-2024-49909,
CVE-2024-49911, CVE-2024-49915, CVE-2024-49917, CVE-2024-49925, CVE-2024-49929,
CVE-2024-49939, CVE-2024-49951, CVE-2024-49994, CVE-2024-49996, CVE-2024-50014,
CVE-2024-50047, CVE-2024-50055, CVE-2024-50121, CVE-2024-50146, CVE-2024-50164,
CVE-2024-50248, CVE-2024-50258, CVE-2024-50275, CVE-2024-50304, CVE-2024-53099,
CVE-2024-53105, CVE-2024-53124, CVE-2024-53125, CVE-2024-53128, CVE-2024-53141,
CVE-2024-53142, CVE-2024-53164, CVE-2024-53170, CVE-2024-53229, CVE-2024-53240,
CVE-2024-53241, CVE-2024-53685, CVE-2024-56551, CVE-2024-56582, CVE-2024-56599,
CVE-2024-56608, CVE-2024-56631, CVE-2024-56664, CVE-2024-56703, CVE-2024-56709,
CVE-2024-56715, CVE-2024-56718, CVE-2024-56759, CVE-2024-57887, CVE-2024-57892,
CVE-2024-57907) (Bug #57930, Bug #57948)
 - **nvidia-graphics-drivers** (CVE-2024-0126) (Bug #57925)
 - **openjpeg2** (CVE-2021-3575, CVE-2023-39327, CVE-2024-56826, CVE-2024-56827) (Bug #57928)
 - **python-tornado** (CVE-2023-28370, CVE-2024-52804) (Bug #57918)
 - **python-urllib3** (CVE-2023-43804, CVE-2023-45803, CVE-2024-37891) (Bug #57931)
 - **python3.11** (CVE-2023-27043, CVE-2024-11168, CVE-2024-6923, CVE-2024-7592,
CVE-2024-9287) (Bug #57915)
 - **qemu** (CVE-2024-7409) (Bug #57922)
 - **rsync** (CVE-2024-12084, CVE-2024-12085, CVE-2024-12086, CVE-2024-12087,

CVE-2024-12088, CVE-2024-12747) (Bug #57932)

- **setuptools** (CVE-2024-6345) (Bug #57917)
- **tiff** (CVE-2023-25433, CVE-2023-26965, CVE-2023-26966, CVE-2023-2908, CVE-2023-3618, CVE-2023-52356, CVE-2024-7006) (Bug #57921)
- **util-linux** (CVE-2024-28085) (Bug #57929)
- **xen** (CVE-2023-28746, CVE-2023-46841, CVE-2023-46842, CVE-2024-2193, CVE-2024-2201, CVE-2024-31142, CVE-2024-31143, CVE-2024-31145, CVE-2024-31146, CVE-2024-45817, CVE-2024-45818, CVE-2024-45819) (Bug #57912)

- Univention Corporate Server 5.2-1 includes the following updated packages from Debian 12:

```
emacs xorg-server base-files criu debootstrap espeak-ng nfs-utils systemd tz-  
data ucf allow-html-temp ansible-core audiofile bochs cacti chromium cpuinfo  
debian-installer debian-installer-netboot-images debian-security-support  
dnsmasq dpdkg eas4tbsyncg fastnetmong geoclue-2.0g git-lfs grml-rescue-  
bootg gst-plugins-base1.0g gst-plugins-good1.0g gstreamer1.0g gunicorn  
icinga2g lemonldap-ngg libebmlg libpgjavag libreofficeg libxstream-javag  
live-bootg llvm-toolchain-19g lxcg mailmindrg nvidia-open-gpu-kernel-mod-  
ulesg oarg openafsgopenh264g openjdk-17g openscg pam-pkcs11g pam-u2fg  
pdns-recursorpg pgtclg pocog prometheus-node-exporter-collectorsg pypy3g  
python-asyncsshg python-werkzeugg quicktextg redisg renderdocg ruby-door-  
keeperg snapcastg sqlparseg srtg tangog tbsyncg texlive-bing thunderbirdg  
tomcat10g webkit2gtk xsaneg zfs-linuxg zookeeperg
```


UNIVENTION MANAGEMENT CONSOLE

2.1 User management

- Added the Message-ID header to emails sent through Self Service to prevent rejection by certain email providers (Bug #57512).

SOFTWARE DEPLOYMENT

- Fixed the link to the 5.2 changelog for the pre-update check ([Bug #57973](#)).

SYSTEM SERVICES

4.1 SAML

- Fixed an issue that causes `univention-keycloak` to crash on system that were not running UCR (Bug #57964).
- Fixed the link to the 5.2 changelog in `univention-keycloak-migration-status` (Bug #57973).

4.2 Proxy services

- You can now manually configure the squid cache settings. Any value other than `ufs` in the UCR variable `squid/cache/format` deactivates the cache configuration in `squid.conf`. You can add a custom squid cache configuration to the `/etc/squid/local.conf` file (Bug #57775).

INDEX

B

Bugzilla

Bug #57512, 5
Bug #57775, 9
Bug #57911, 1
Bug #57912, 3
Bug #57913, 2
Bug #57914, 1
Bug #57915, 2
Bug #57916, 1
Bug #57917, 3
Bug #57918, 2
Bug #57919, 1
Bug #57920, 1
Bug #57921, 3
Bug #57922, 2
Bug #57923, 1
Bug #57924, 1
Bug #57925, 2
Bug #57926, 1
Bug #57927, 1
Bug #57928, 2
Bug #57929, 3
Bug #57930, 2
Bug #57931, 2
Bug #57932, 3
Bug #57948, 2
Bug #57950, 1
Bug #57964, 9
Bug #57966, 1
Bug #57969, 1
Bug #57973, 7, 9

C

CVE

CVE-2020-35357, 1
CVE-2021-3575, 2
CVE-2022-49034, 1
CVE-2023-2908, 3
CVE-2023-3618, 3
CVE-2023-25433, 3
CVE-2023-26965, 3
CVE-2023-26966, 3
CVE-2023-27043, 2
CVE-2023-28370, 2
CVE-2023-28746, 3

CVE-2023-38469, 1
CVE-2023-38470, 1
CVE-2023-38471, 1
CVE-2023-38472, 1
CVE-2023-38473, 1
CVE-2023-39327, 2
CVE-2023-43804, 2
CVE-2023-45803, 2
CVE-2023-46841, 3
CVE-2023-46842, 3
CVE-2023-52356, 3
CVE-2023-52916, 1, 2
CVE-2024-0126, 2
CVE-2024-2193, 3
CVE-2024-2201, 3
CVE-2024-6345, 3
CVE-2024-6923, 2
CVE-2024-7006, 3
CVE-2024-7409, 2
CVE-2024-7592, 2
CVE-2024-9287, 2
CVE-2024-11168, 2
CVE-2024-11187, 1
CVE-2024-11704, 1
CVE-2024-12084, 2
CVE-2024-12085, 2
CVE-2024-12086, 2
CVE-2024-12087, 2
CVE-2024-12088, 3
CVE-2024-12133, 1
CVE-2024-12243, 1
CVE-2024-12705, 1
CVE-2024-12747, 3
CVE-2024-21820, 1
CVE-2024-21853, 1
CVE-2024-22195, 1
CVE-2024-23918, 1
CVE-2024-26595, 1
CVE-2024-27407, 1, 2
CVE-2024-28085, 3
CVE-2024-31142, 3
CVE-2024-31143, 3
CVE-2024-31145, 3
CVE-2024-31146, 3
CVE-2024-34064, 1
CVE-2024-35870, 1, 2

CVE-2024-35956, 1, 2	CVE-2024-53099, 1, 2
CVE-2024-36479, 1, 2	CVE-2024-53105, 1, 2
CVE-2024-36899, 1, 2	CVE-2024-53124, 1, 2
CVE-2024-37021, 1, 2	CVE-2024-53125, 1, 2
CVE-2024-37891, 2	CVE-2024-53128, 1, 2
CVE-2024-41014, 1, 2	CVE-2024-53141, 1, 2
CVE-2024-42252, 1, 2	CVE-2024-53142, 1, 2
CVE-2024-42315, 1, 2	CVE-2024-53145, 1
CVE-2024-42319, 1	CVE-2024-53146, 1
CVE-2024-43098, 1	CVE-2024-53148, 1
CVE-2024-44950, 1, 2	CVE-2024-53150, 1
CVE-2024-45817, 3	CVE-2024-53151, 1
CVE-2024-45818, 3	CVE-2024-53154, 1
CVE-2024-45819, 3	CVE-2024-53155, 1
CVE-2024-45828, 1	CVE-2024-53156, 1
CVE-2024-46809, 1, 2	CVE-2024-53157, 1
CVE-2024-46841, 1	CVE-2024-53158, 1
CVE-2024-46896, 1	CVE-2024-53161, 1
CVE-2024-47143, 1	CVE-2024-53164, 1, 2
CVE-2024-47408, 1	CVE-2024-53165, 1
CVE-2024-47745, 1	CVE-2024-53170, 1, 2
CVE-2024-48881, 1	CVE-2024-53171, 1
CVE-2024-49571, 1	CVE-2024-53172, 1
CVE-2024-49861, 1, 2	CVE-2024-53173, 1
CVE-2024-49891, 1, 2	CVE-2024-53174, 1
CVE-2024-49897, 1, 2	CVE-2024-53175, 1
CVE-2024-49898, 1, 2	CVE-2024-53180, 1
CVE-2024-49899, 1, 2	CVE-2024-53181, 1
CVE-2024-49909, 1, 2	CVE-2024-53183, 1
CVE-2024-49911, 1, 2	CVE-2024-53184, 1
CVE-2024-49915, 1, 2	CVE-2024-53190, 1
CVE-2024-49917, 1, 2	CVE-2024-53194, 1
CVE-2024-49925, 1, 2	CVE-2024-53196, 1
CVE-2024-49929, 1, 2	CVE-2024-53197, 1
CVE-2024-49934, 1	CVE-2024-53198, 1
CVE-2024-49939, 1, 2	CVE-2024-53206, 1
CVE-2024-49951, 1, 2	CVE-2024-53207, 1
CVE-2024-49994, 1, 2	CVE-2024-53208, 1
CVE-2024-49996, 1, 2	CVE-2024-53210, 1
CVE-2024-50014, 1, 2	CVE-2024-53213, 1
CVE-2024-50047, 1, 2	CVE-2024-53214, 1
CVE-2024-50051, 1	CVE-2024-53215, 1
CVE-2024-50055, 1, 2	CVE-2024-53217, 1
CVE-2024-50121, 1, 2	CVE-2024-53220, 1
CVE-2024-50146, 1, 2	CVE-2024-53226, 1
CVE-2024-50164, 1, 2	CVE-2024-53227, 1
CVE-2024-50248, 1, 2	CVE-2024-53229, 1, 2
CVE-2024-50258, 1, 2	CVE-2024-53230, 1
CVE-2024-50275, 1, 2	CVE-2024-53231, 1
CVE-2024-50304, 1, 2	CVE-2024-53233, 1
CVE-2024-50349, 1	CVE-2024-53237, 1
CVE-2024-52006, 1	CVE-2024-53239, 1
CVE-2024-52332, 1	CVE-2024-53240, 1, 2
CVE-2024-52530, 1	CVE-2024-53241, 1, 2
CVE-2024-52531, 1	CVE-2024-53680, 1
CVE-2024-52532, 1	CVE-2024-53685, 1, 2
CVE-2024-52533, 1	CVE-2024-53690, 1
CVE-2024-52804, 2	CVE-2024-55881, 1

CVE-2024-55916, 1	CVE-2024-56630, 2
CVE-2024-56369, 1	CVE-2024-56631, 2
CVE-2024-56531, 1	CVE-2024-56633, 2
CVE-2024-56532, 1	CVE-2024-56634, 2
CVE-2024-56533, 2	CVE-2024-56636, 2
CVE-2024-56539, 2	CVE-2024-56637, 2
CVE-2024-56546, 2	CVE-2024-56640, 2
CVE-2024-56548, 2	CVE-2024-56642, 2
CVE-2024-56551, 2	CVE-2024-56643, 2
CVE-2024-56557, 2	CVE-2024-56644, 2
CVE-2024-56558, 2	CVE-2024-56645, 2
CVE-2024-56562, 2	CVE-2024-56648, 2
CVE-2024-56567, 2	CVE-2024-56650, 2
CVE-2024-56568, 2	CVE-2024-56651, 2
CVE-2024-56569, 2	CVE-2024-56658, 2
CVE-2024-56570, 2	CVE-2024-56659, 2
CVE-2024-56571, 2	CVE-2024-56660, 2
CVE-2024-56572, 2	CVE-2024-56661, 2
CVE-2024-56574, 2	CVE-2024-56662, 2
CVE-2024-56575, 2	CVE-2024-56663, 2
CVE-2024-56576, 2	CVE-2024-56664, 2
CVE-2024-56578, 2	CVE-2024-56665, 2
CVE-2024-56579, 2	CVE-2024-56670, 2
CVE-2024-56581, 2	CVE-2024-56672, 2
CVE-2024-56582, 2	CVE-2024-56675, 2
CVE-2024-56584, 2	CVE-2024-56677, 2
CVE-2024-56585, 2	CVE-2024-56678, 2
CVE-2024-56586, 2	CVE-2024-56679, 2
CVE-2024-56587, 2	CVE-2024-56681, 2
CVE-2024-56589, 2	CVE-2024-56683, 2
CVE-2024-56590, 2	CVE-2024-56687, 2
CVE-2024-56593, 2	CVE-2024-56688, 2
CVE-2024-56594, 2	CVE-2024-56690, 2
CVE-2024-56595, 2	CVE-2024-56691, 2
CVE-2024-56596, 2	CVE-2024-56693, 2
CVE-2024-56597, 2	CVE-2024-56694, 2
CVE-2024-56598, 2	CVE-2024-56698, 2
CVE-2024-56599, 2	CVE-2024-56700, 2
CVE-2024-56600, 2	CVE-2024-56701, 2
CVE-2024-56601, 2	CVE-2024-56703, 2
CVE-2024-56602, 2	CVE-2024-56704, 2
CVE-2024-56603, 2	CVE-2024-56705, 2
CVE-2024-56604, 2	CVE-2024-56707, 2
CVE-2024-56605, 2	CVE-2024-56708, 2
CVE-2024-56606, 2	CVE-2024-56709, 2
CVE-2024-56608, 2	CVE-2024-56715, 2
CVE-2024-56610, 2	CVE-2024-56716, 2
CVE-2024-56614, 2	CVE-2024-56717, 2
CVE-2024-56615, 2	CVE-2024-56718, 2
CVE-2024-56616, 2	CVE-2024-56720, 2
CVE-2024-56619, 2	CVE-2024-56722, 2
CVE-2024-56622, 2	CVE-2024-56723, 2
CVE-2024-56623, 2	CVE-2024-56724, 2
CVE-2024-56625, 2	CVE-2024-56725, 2
CVE-2024-56626, 2	CVE-2024-56726, 2
CVE-2024-56627, 2	CVE-2024-56727, 2
CVE-2024-56628, 2	CVE-2024-56728, 2
CVE-2024-56629, 2	CVE-2024-56739, 2

CVE-2024-56741, 2
CVE-2024-56745, 2
CVE-2024-56746, 2
CVE-2024-56747, 2
CVE-2024-56748, 2
CVE-2024-56751, 2
CVE-2024-56754, 2
CVE-2024-56755, 2
CVE-2024-56756, 2
CVE-2024-56759, 2
CVE-2024-56763, 2
CVE-2024-56765, 2
CVE-2024-56766, 2
CVE-2024-56767, 2
CVE-2024-56769, 2
CVE-2024-56770, 2
CVE-2024-56774, 2
CVE-2024-56776, 2
CVE-2024-56777, 2
CVE-2024-56778, 2
CVE-2024-56779, 2
CVE-2024-56780, 2
CVE-2024-56781, 2
CVE-2024-56783, 2
CVE-2024-56785, 2
CVE-2024-56787, 2
CVE-2024-56826, 2
CVE-2024-56827, 2
CVE-2024-57791, 2
CVE-2024-57792, 2
CVE-2024-57798, 2
CVE-2024-57807, 2
CVE-2024-57838, 2
CVE-2024-57849, 2
CVE-2024-57850, 2
CVE-2024-57874, 2
CVE-2024-57876, 2
CVE-2024-57887, 2
CVE-2024-57892, 2
CVE-2024-57907, 2
CVE-2024-57946, 2
CVE-2025-0237, 1
CVE-2025-0238, 1
CVE-2025-0239, 1
CVE-2025-0240, 1
CVE-2025-0241, 1
CVE-2025-0242, 1
CVE-2025-0243, 1
CVE-2025-1009, 1
CVE-2025-1010, 1
CVE-2025-1011, 1
CVE-2025-1012, 1
CVE-2025-1013, 1
CVE-2025-1014, 1
CVE-2025-1016, 1
CVE-2025-1017, 1

E

environment variable
squid/cache/format, 9

S

squid/cache/format, 9