



V3.1.403 BSP UN60, UN65, UN78

Release Notes

BSP Release Notes

Platform details

Platform	BSP ID	Previous	Current
VL-704 SMART VL-707 SMART VL-710 SMART VL-700 BASE	UN60	1.3.718	3.1.403
VL-707 STYLE VL-710 STYLE	UN65	1.3.836	3.1.403

Items in this table are classified as:

- F Feature implementation of a new feature.
- B Bug solution to problems reported by users. Summary may include the Case ID number assigned during technical support.
- S Security Implementation related to cyber-security; may include features or bugs.
- C CVE Implementation of CVE

BSP packages are available for download at <https://deuta-controls.net/iot-infrastruktur/enoccean-gateway-vl-700-base/> only after official release to production.

Version	Ticket ID	Type	Summary	UN60	UN65	UN78	Notes
	BSP-5781	Bug	Installation of large apps may fail due to insufficient space also when not true	•	•	•	
	BSP-5637	Bug	FTP server cannot be used through a NAT rule - Case ID: 202400535	•	•	•	
	BSP-5540	Bug	UN78 Improve CAN interfaces real-time performance			•	
	BSP-5277	Bug	eX707 loses responses to RTR CANopen messages occasionally		•	•	
	BSP-5239	Bug	DNS servers are not saved if firewall or static IPs are enabled	•	•	•	
	BSP-5021	Bug	HMI freezes when using MPI protocol with serial plugin modules - Case ID: 202302120	•	•	•	
	BSP-4711	Bug	Cloud VPN does not reset last valid connection	•	•	•	
	BSP-4666	Bug	Network DNS entry cannot be removed	•	•	•	
	BSP-4662	Bug	Touch does not work properly when we switch from auto detect display orientation at boot		•	•	
	BSP-3275	Bug	High memory usage after pressure test on VNC server	•	•	•	
	BSP-3275	Bug	VNC service limited to maximum 10 simultaneous client connections	•	•	•	
	BSP-3274	Bug	Web management interface does not work if data partition is full	•	•	•	
	BSP-3261	Bug	Q and A keys are inverted in the French keyboard layout	•	•	•	
	BSP-3221	Bug	Network restart takes 50 sec when mobile is enabled + fix empty reg stat	•	•	•	
	BSP-3186	Bug	Graphical issues on VNC using tight encoding	•	•	•	
	BSP-2979	Bug	Issues with temporary storage tmpfs	•	•	•	
	BSP-6154	Feature	Add legal section in SystemSettings	•	•	•	
	BSP-5865	Feature	Add option in System Settings to disable GPU g2d for browser panels			•	
	BSP-5522	Feature	Fixed issues with NTP Server	•	•	•	
	BSP-5513	Feature	Add support for new display eX710-eX710M	•	•	•	
	BSP-5476	Feature	Extends the Firewall Service to allow the specified domains to be whitelisted or blacklisted	•	•	•	
	BSP-4861	Feature	Cloud Agent configuration via machine.ini	•	•	•	
	BSP-478	Feature	UN6x: Make network interface priorities configurable (metric)	•	•	•	
	BSP-4584	Feature	Disable kernel magic keys support	•	•	•	
	BSP-3384	Feature	FRAM Backup / Restore from USB updater, System Settings and Manage Target in JMobile		•	•	

Version	Ticket ID	Type	Summary	UN60	UN65	UN78	Notes
	BSP-3293	Feature	Improve video player performance on i.MX6 eX700 / JSmart700		•		
	BSP-3262	Feature	LED control REST API		•	•	
	BSP-3232	Feature	Reduce the number of supported multimedia codecs	•	•	•	
	BSP-3101	Feature	Add Mono Yocto layer	•	•	•	
	BSP-2795	Feature	IEEE 802.1x wired support - Case ID: 202104334	•	•	•	
	BSP-2109	Feature	Update to QT5.15	•	•	•	
	BSP-1635	Feature	Support for installing Docker Application and related containers	•	•	•	
	BSP-5618	S	CORS are enabled even if disabled from System Settings	•	•	•	
	BSP-5617	S	Enable Content Security Policy (CSP) for System Settings	•	•	•	
	BSP-4627	S	Add option to disable external USB devices in system settings	•	•	•	
	BSP-3428	S	CA-certificates are installed on a non-standard path	•	•	•	
	BSP-3237	S	Add ssh client to ConfigOS image	•	•	•	
	BSP-3149	S	In VNC settings page, every time when we edit and save, ask user to enter password	•	•	•	
	BSP-3140	S	Make sure OpenSSL libraries accept only TLS version 1.2 or greater	•	•	•	
	BSP-3088	S	Set SameSite=strict for all cookies	•	•	•	
	BSP-3055	S	In Security page, add reauthorization before showing the stored password	•	•	•	
	BSP-3025	S	Disable user "user" by default	•	•	•	
	BSP-2923	S	Update openssh to 9.6	•	•	•	
	BSP-2425	S	Implement loading custom VNC server certificate	•	•	•	
	BSP-1844	S	Include HTTP Strict-Transport-Security headers in HTTPS responses	•	•	•	
	BSP-1823	S	Implement account lockout or authentication throttling and random delays. Protection against Brute Force Attacks	•	•	•	
	BSP-1817	S	Enforce idle and absolute session timeouts	•	•	•	
	BSP-1816	S	Implement cookie-based authentication sessions	•	•	•	
	BSP-1815	S	Use anti-Cross-Site Request Forgery (CSRF) tokens	•	•	•	
	BSP-5926	C	CVE-2024-6387	•	•	•	
	BSP-5863	C	CVE-2021-3520	•	•	•	
	BSP-5805	C	CVE-2023-48795 (SSH Terrapin Prefix Truncation Weakness)	•	•	•	
	BSP-5736	C	CVE-2021-47194	•	•	•	
	BSP-5715	C	CVE-2019-25162	•	•	•	
	BSP-5687	C	C-2021-46936	•	•	•	

Version	Ticket ID	Type	Summary	UN60	UN65	UN78	Notes
	BSP-5663	C	C-2023-52449	•	•	•	
	BSP-5630	C	C-2024-25739	•	•	•	
	BSP-5620	C	C-2023-50387	•	•	•	
	BSP-5599	C	C-2024-25062	•	•	•	
	BSP-5585	C	C-2024-1086	•	•	•	
	BSP-5575	C	C-2023-52356	•	•	•	
	BSP-5574	C	C-2023-52355	•	•	•	
	BSP-5571	C	C-2024-0409	•	•	•	
	BSP-5565	C	C-2023-42915	•	•	•	
	BSP-5557	C	C-2024-0775	•	•	•	
	BSP-5555	C	C-2024-0607	•	•	•	
	BSP-5554	C	C-2023-6816	•	•	•	
	BSP-5549	C	C-2024-0567	•	•	•	
	BSP-5547	C	C-2024-0553	•	•	•	
	BSP-5534	C	C-2023-6004	•	•	•	
	BSP-5532	C	C-2022-48619	•	•	•	
	BSP-5526	C	C-2022-2586	•	•	•	
	BSP-5509	C	C-2023-6228	•	•	•	
	BSP-5508	C	C-2023-51384	•	•	•	
	BSP-5507	C	C-2023-48795	•	•	•	
	BSP-5506	C	CVE-2023-51385	•	•	•	
	BSP-5505	C	CVE-2023-42465	•	•	•	
	BSP-5504	C	C-2023-6932	•	•	•	
	BSP-5500	C	C-2023-35001	•	•	•	
	BSP-5499	C	C-2023-51714	•	•	•	
	BSP-5498	C	CVE-2023-7104	•	•	•	
	BSP-5492	C	C-2023-46219	•	•	•	
	BSP-5468	C	C-2023-46218	•	•	•	
	BSP-5454	C	C-2023-6277	•	•	•	
	BSP-5411	C	C-2023-38473	•	•	•	
	BSP-5410	C	C-2023-38472	•	•	•	
	BSP-5409	C	C-2023-38471	•	•	•	
	BSP-5408	C	C-2023-38470	•	•	•	
	BSP-5407	C	C-2023-38469	•	•	•	
	BSP-5384	C	CVE-2023-38546	•	•	•	
	BSP-5383	C	C-2023-3338	•	•	•	
	BSP-5381	C	CVE-2023-38545	•	•	•	
	BSP-5374	C	C-2023-45863	•	•	•	
	BSP-5370	C	CVE-2023-45871	•	•	•	
	BSP-5369	C	CVE-2023-45853	•	•	•	
	BSP-5368	C	C-2023-42752	•	•	•	
	BSP-5367	C	C-2023-44487	•	•	•	

Version	Ticket ID	Type	Summary	UN60	UN65	UN78	Notes
	BSP-5363	C	CVE-2023-39194	•	•	•	
	BSP-5362	C	CVE-2023-43786	•	•	•	
	BSP-5361	C	CVE-2023-43785	•	•	•	
	BSP-5360	C	CVE-2023-42754	•	•	•	
	BSP-5355	C	CVE-2023-45322	•	•	•	
	BSP-5354	C	CVE-2023-43787	•	•	•	
	BSP-5345	C	CVE-2023-41175 (tiff)	•	•	•	
	BSP-5344	C	CVE-2023-40745 (tiff)	•	•	•	
	BSP-5337	C	CVE-2023-4911 (glibc)	•	•	•	
	BSP-5333	C	CVE-2019-19447 (linux-imx-rt)	•	•	•	
	BSP-5331	C	CVE-2023-5197 (linux-imx-rt)	•	•	•	
	BSP-5321	C	CVE-2019-18397 (fribidi)	•	•	•	
	BSP-5320	C	CVE-2022-25308 (fribidi)	•	•	•	
	BSP-5317	C	CVE-2023-43114 (qtbase)	•	•	•	
	BSP-5316	C	CVE-2023-32611 (glib-2.0)	•	•	•	
	BSP-5313	C	CVE-2023-4156 (gawk)	•	•	•	
	BSP-5312	C	CVE-2023-5156 (glibc)	•	•	•	
	BSP-5311	C	CVE-2023-38039 (curl)	•	•	•	
	BSP-5310	C	CVE-2023-32643 (glib-2.0)	•	•	•	
	BSP-5303	C	C-2020-36766 (linux-imx-rt)	•	•	•	
	BSP-5302	C	CVE-2023-32665 (glib-2.0)	•	•	•	
	BSP-5300	C	CVE-2023-32636 (glib-2.0)	•	•	•	
	BSP-5299	C	CVE-2023-29499 (glib-2.0)	•	•	•	
	BSP-5298	C	CVE-2023-4813 (glibc)	•	•	•	
	BSP-5296	C	CVE-2023-3777 (linux-imx-rt)	•	•	•	
	BSP-5294	C	CVE-2023-4863 (libwebp)	•	•	•	
	BSP-5287	C	CVE-2023-4881 (linux-imx-rt)	•	•	•	
	BSP-5284	C	CVE-2023-40217 (python3)	•	•	•	
	BSP-5283	C	CVE-2023-4244 (linux-imx-rt)	•	•	•	
	BSP-5282	C	CVE-2023-4622 (linux-imx-rt)	•	•	•	
	BSP-5281	C	CVE-2023-4015 (linux-imx-rt)	•	•	•	
	BSP-5266	C	CVE-2022-48174 (busybox)	•	•	•	
	BSP-5262	C	CVE-2022-40090 (tiff)	•	•	•	
	BSP-5261	C	CVE-2021-32292 (json-c)	•	•	•	
	BSP-5260	C	CVE-2020-22219 (flac)	•	•	•	
	BSP-5248	C	CVE-2020-21047 (elfutils)	•	•	•	
	BSP-5246	C	CVE-2023-37369 (qtbase)	•	•	•	
	BSP-5230	C	CVE-2023-4273 (linux-ti)	•	•	•	
	BSP-5227	C	CVE-2023-4147 (linux-ti)	•	•	•	
	BSP-5216	C	CVE-2023-3817 (openssl)	•	•	•	
	BSP-5211	C	CVE-2023-38408 (openssh)	•	•	•	
	BSP-5207	C	CVE-2023-3773 (linux-imx-rt)	•	•	•	

Version	Ticket ID	Type	Summary	UN60	UN65	UN78	Notes
	BSP-5205	C	CVE-2023-32001 (curl)	•	•	•	
	BSP-5204	C	C-2023-4016 (procps)	•	•	•	
	BSP-5203	C	CVE-2022-1729 (linux-imx-rt)	•	•	•	
	BSP-5201	C	CVE-2023-3610 (linux-imx-rt)	•	•	•	
	BSP-5200	C	CVE-2023-4004 (linux-imx-rt)	•	•	•	
	BSP-5196	C	CVE-2023-3863 (linux-ti)	•	•	•	
	BSP-5195	C	CVE-2023-3772 (linux-ti)	•	•	•	
	BSP-5190	C	CVE-2023-3567 (linux-ti)	•	•	•	
	BSP-5186	C	CVE-2023-3812 (linux-ti)	•	•	•	
	BSP-5175	C	CVE-2022-33065 (libsndfile1)	•	•	•	
	BSP-5162	C	CVE-2023-38197 (qtbases)	•	•	•	
	BSP-5161	C	CVE-2022-41409 (libpcre2)	•	•	•	
	BSP-5154	C	CVE-2020-16135 (libssh)	•	•	•	
	BSP-5153	C	CVE-2023-3618 (tiff)	•	•	•	
	BSP-5152	C	CVE-2022-25636 (linux-imx-rt)	•	•	•	
	BSP-5147	C	CVE-2022-3553 (xserver-xorg)	•	•	•	
	BSP-5145	C	CVE-2020-29074 (x11vnc)	•	•	•	
	BSP-5100	C	CVE-2021-3502 (avahi)	•	•	•	
	BSP-5076	C	CVE-2023-26551 (ntp)	•	•	•	
	BSP-5075	C	CVE-2023-26554 (ntp)	•	•	•	
	BSP-5074	C	CVE-2023-26552 (ntp)	•	•	•	
	BSP-5073	C	CVE-2023-26553 (ntp)	•	•	•	
	BSP-5061	C	CVE-2023-26555 (ntp)	•	•	•	
	BSP-5060	C	CVE-2023-34969 (dbus)	•	•	•	
	BSP-5055	C	CVE-2023-1295 (linux-imx-rt)	•	•	•	
	BSP-5053	C	CVE-2022-26488 (python3)	•	•	•	
	BSP-5051	C	CVE-2023-0361 (gnutls)	•	•	•	
	BSP-5040	C	CVE-2023-36632 (python3)	•	•	•	
	BSP-5037	C	CVE-2022-30065 (busybox)	•	•	•	
	BSP-5027	C	CVE-2021-41072 (squashfs-tools)	•	•	•	
	BSP-5023	C	C-2023-0687 (glibc)	•	•	•	
	BSP-5022	C	CVE-2022-1664 (dpkg)	•	•	•	
	BSP-5011	C	CVE-2023-31124 (c-ares)	•	•	•	
	BSP-5010	C	CVE-2023-37453 (linux-ti)	•	•	•	
	BSP-5002	C	CVE-2023-37454 (linux-ti)	•	•	•	
	BSP-5000	C	CVE-2023-1206 (linux-ti)	•	•	•	
	BSP-4999	C	CVE-2023-31130 (c-ares)	•	•	•	
	BSP-4998	C	CVE-2023-31147 (c-ares)	•	•	•	
	BSP-4997	C	CVE-2023-32067 (c-ares)	•	•	•	
	BSP-4996	C	CVE-2023-3138 (libx11)	•	•	•	
	BSP-4993	C	CVE-2023-3390 (linux-ti)	•	•	•	
	BSP-4991	C	CVE-2022-4904 (c-ares)	•	•	•	

Version	Ticket ID	Type	Summary	UN60	UN65	UN78	Notes
	BSP-4987	C	CVE-2023-1999 (libwebp)	•	•	•	
	BSP-4984	C	CVE-2023-36191 (sqlite3)	•	•	•	
	BSP-4983	C	CVE-2023-3316 (tiff)	•	•	•	
	BSP-4976	C	CVE-2023-26965 (tiff)	•	•	•	
	BSP-4975	C	CVE-2023-25435 (tiff)	•	•	•	
	BSP-4965	C	CVE-2023-25434 (tiff)	•	•	•	
	BSP-4955	C	CVE-2023-3161 (linux-imx-rt)	•	•	•	
	BSP-4954	C	CVE-2023-2603 (libcap)	•	•	•	
	BSP-4950	C	CVE-2023-34410 (qtbase)	•	•	•	
	BSP-4935	C	CVE-2023-32762 (qtbase)	•	•	•	
	BSP-4933	C	CVE-2023-28320 (curl)	•	•	•	
	BSP-4932	C	CVE-2023-2804 (libjpeg-turbo)	•	•	•	
	BSP-4931	C	CVE-2023-32763 (qtbase)	•	•	•	
	BSP-4930	C	CVE-2023-33285 (qtbase)	•	•	•	
	BSP-4929	C	CVE-2023-28319 (curl)	•	•	•	
	BSP-4928	C	CVE-2023-28321 (curl)	•	•	•	
	BSP-4927	C	CVE-2023-2650 (openssl)	•	•	•	
	BSP-4926	C	CVE-2023-28322 (curl)	•	•	•	
	BSP-4921	C	CVE-2023-33203 (linux-imx-rt)	•	•	•	
	BSP-4913	C	CVE-2023-29383 (shadow)	•	•	•	
	BSP-4911	C	CVE-2023-0458 (linux-ti)	•	•	•	
	BSP-4909	C	CVE-2023-1582 (linux-ti)	•	•	•	
	BSP-4904	C	CVE-2023-2166 (linux-ti)	•	•	•	
	BSP-4901	C	CVE-2023-1916 (tiff)	•	•	•	
	BSP-4898	C	CVE-2023-29469 (libxml2)	•	•	•	
	BSP-4897	C	CVE-2023-28484 (libxml2)	•	•	•	
	BSP-4896	C	CVE-2023-2513 (linux-ti)	•	•	•	
	BSP-4888	C	CVE-2023-32573 (qtsvg)	•	•	•	
	BSP-4887	C	CVE-2023-24607 (qtbase)	•	•	•	
	BSP-4886	C	CVE-2023-1393 (xserver-xorg)	•	•	•	
	BSP-4884	C	CVE-2023-32233 (linux-ti)	•	•	•	
	BSP-4883	C	CVE-2023-29491 (ncurses)	•	•	•	
	BSP-4882	C	CVE-2023-1829 (linux-ti)	•	•	•	
	BSP-4852	C	CVE-2022-2978 (linux-imx-rt)	•	•	•	
	BSP-4841	C	CVE-2023-27538 (curl)	•	•	•	
	BSP-4840	C	CVE-2023-1076 (linux-ti)	•	•	•	
	BSP-4837	C	CVE-2023-27535 (curl)	•	•	•	
	BSP-4835	C	CVE-2022-48434 (ffmpeg)	•	•	•	
	BSP-4834	C	CVE-2023-27534 (curl)	•	•	•	
	BSP-4833	C	CVE-2023-27533 (curl)	•	•	•	
	BSP-4832	C	CVE-2023-27536 (curl)	•	•	•	
	BSP-4826	C	CVE-2023-0465 (openssl)	•	•	•	

Version	Ticket ID	Type	Summary	UN60	UN65	UN78	Notes
	BSP-4822	C	CVE-2023-1073 (linux-imx-rt)	•	•	•	
	BSP-4821	C	CVE-2023-1380 (linux-imx-rt)	•	•	•	
	BSP-4817	C	CVE-2023-1077 (linux-imx-rt)	•	•	•	
	BSP-4808	C	CVE-2023-0590 (linux-imx-rt)	•	•	•	
	BSP-4807	C	CVE-2023-1249 (linux-imx-rt)	•	•	•	
	BSP-4805	C	CVE-2023-0464 (openssl)	•	•	•	
	BSP-4795	C	CVE-2023-0386 (linux-imx-rt)	•	•	•	
	BSP-4794	C	CVE-2023-28772 (linux-imx-rt)	•	•	•	
	BSP-4785	C	CVE-2023-28487 (sudo)	•	•	•	
	BSP-4784	C	CVE-2023-28486 (sudo)	•	•	•	
	BSP-4782	C	CVE-2023-28450 (dnsmasq)	•	•	•	
	BSP-4780	C	CVE-2023-28531 (openssh)	•	•	•	
	BSP-4771	C	CVE-2023-23004 (linux-ti)	•	•	•	
	BSP-4770	C	CVE-2023-27320 (sudo)	•	•	•	
	BSP-4768	C	CVE-2023-0461 (linux-ti)	•	•	•	
	BSP-4745	C	CVE-2020-24588 (linux-ti)	•	•	•	
	BSP-4740	C	CVE-2023-1095 (linux-ti)	•	•	•	
	BSP-4733	C	CVE-2023-23915 (curl)	•	•	•	
	BSP-4728	C	CVE-2023-23916 (curl)	•	•	•	
	BSP-4726	C	CVE-2021-3760 (linux-ti)	•	•	•	
	BSP-4724	C	CVE-2023-23000 (linux-ti)	•	•	•	
	BSP-4713	C	CVE-2023-23914 (curl)	•	•	•	
	BSP-4695	C	CVE-2022-4304 (openssl)	•	•	•	
	BSP-4687	C	CVE-2023-0286 (openssl)	•	•	•	
	BSP-4686	C	CVE-2022-4450 (openssl)	•	•	•	
	BSP-4685	C	CVE-2023-0215 (openssl)	•	•	•	
	BSP-4680	C	CVE-2023-25193 (harfbuzz)	•	•	•	
	BSP-4674	C	CVE-2023-0394 (linux-ti)	•	•	•	
	BSP-4672	C	CVE-2022-48303 (tar)	•	•	•	
	BSP-4670	C	CVE-2023-0266 (linux-ti)	•	•	•	
	BSP-4655	C	CVE-2022-48281 (tiff)	•	•	•	
	BSP-4653	C	CVE-2022-3341 (ffmpeg)	•	•	•	
	BSP-4652	C	CVE-2023-22809 (sudo)	•	•	•	
	BSP-4642	C	CVE-2022-47929 (linux-imx-rt)	•	•	•	
	BSP-4640	C	CVE-2022-4743 (libsdl2)	•	•	•	
	BSP-4637	C	CVE-2022-2964 (linux-imx-rt)	•	•	•	
	BSP-4636	C	CVE-2022-2639 (linux-imx-rt)	•	•	•	
	BSP-4625	C	CVE-2020-16294 (ghostscript)	•	•	•	
	BSP-4624	C	CVE-2020-16295 (ghostscript)	•	•	•	
	BSP-4623	C	CVE-2020-16296 (ghostscript)	•	•	•	
	BSP-4622	C	CVE-2020-16297 (ghostscript)	•	•	•	
	BSP-4621	C	CVE-2020-16287 (ghostscript)	•	•	•	

Version	Ticket ID	Type	Summary	UN60	UN65	UN78	Notes
	BSP-4620	C	CVE-2020-16298 (ghostscript)	•	•	•	
	BSP-4619	C	CVE-2018-16435 (lcms)	•	•	•	
	BSP-4618	C	CVE-2020-16299 (ghostscript)	•	•	•	
	BSP-4617	C	CVE-2020-16288 (ghostscript)	•	•	•	
	BSP-4616	C	CVE-2020-16289 (ghostscript)	•	•	•	
	BSP-4615	C	CVE-2020-16290 (ghostscript)	•	•	•	
	BSP-4614	C	CVE-2020-16291 (ghostscript)	•	•	•	
	BSP-4613	C	CVE-2020-16300 (ghostscript)	•	•	•	
	BSP-4612	C	CVE-2020-16292 (ghostscript)	•	•	•	
	BSP-4611	C	CVE-2020-16293 (ghostscript)	•	•	•	
	BSP-4610	C	CVE-2020-16301 (ghostscript)	•	•	•	
	BSP-4609	C	CVE-2020-16308 (ghostscript)	•	•	•	
	BSP-4608	C	CVE-2020-27792 (ghostscript)	•	•	•	
	BSP-4607	C	CVE-2016-10165 (lcms)	•	•	•	
	BSP-4606	C	CVE-2019-14811 (ghostscript)	•	•	•	
	BSP-4605	C	CVE-2019-14817 (ghostscript)	•	•	•	
	BSP-4604	C	CVE-2019-14812 (ghostscript)	•	•	•	
	BSP-4603	C	CVE-2022-38784 (poppler)	•	•	•	
	BSP-4602	C	CVE-2022-38171 (poppler)	•	•	•	
	BSP-4601	C	CVE-2021-30860 (poppler)	•	•	•	
	BSP-4600	C	CVE-2019-10216 (ghostscript)	•	•	•	
	BSP-4599	C	CVE-2019-14869 (ghostscript)	•	•	•	
	BSP-4598	C	CVE-2019-14813 (ghostscript)	•	•	•	
	BSP-4593	C	CVE-2008-1033 (cups)	•	•	•	
	BSP-4592	C	CVE-2021-25317 (cups)	•	•	•	
	BSP-4591	C	CVE-2022-26691 (cups)	•	•	•	
	BSP-4590	C	CVE-2018-6553 (cups)	•	•	•	
	BSP-4579	C	CVE-2022-4662 (linux-imx-rt)	•	•	•	
	BSP-4576	C	CVE-2022-43551 (curl)	•	•	•	
	BSP-4574	C	CVE-2022-3715 (bash)	•	•	•	
	BSP-4554	C	CVE-2022-3115 (linux-ti)	•	•	•	
	BSP-4552	C	CVE-2022-3109 (ffmpeg)	•	•	•	
	BSP-4548	C	CVE-2022-3964 (ffmpeg)	•	•	•	
	BSP-4546	C	CVE-2022-4603 (ppp)	•	•	•	
	BSP-4530	C	CVE-2022-35260 (curl)	•	•	•	
	BSP-4529	C	CVE-2022-46908 (sqlite3)	•	•	•	
	BSP-4528	C	CVE-2022-32221 (curl)	•	•	•	
	BSP-4507	C	CVE-2022-40303 (libxml2)	•	•	•	
	BSP-4505	C	CVE-2022-40304 (libxml2)	•	•	•	
	BSP-4502	C	CVE-2022-3970 (tiff)	•	•	•	
	BSP-4481	C	CVE-2022-44793 (net-snmp)	•	•	•	
	BSP-4480	C	CVE-2022-44792 (net-snmp)	•	•	•	

Version	Ticket ID	Type	Summary	UN60	UN65	UN78	Notes
	BSP-4479	C	CVE-2022-43945 (linux-imx-rt)	•	•	•	
	BSP-4478	C	CVE-2022-44638 (pixman)	•	•	•	
	BSP-4465	C	CVE-2022-43995 (sudo)	•	•	•	
	BSP-4464	C	CVE-2022-2053 (tiff)	•	•	•	
	BSP-4463	C	CVE-2021-36690 (sqlite3)	•	•	•	
	BSP-4462	C	CVE-2022-42916 (curl)	•	•	•	
	BSP-4459	C	CVE-2022-42915 (curl)	•	•	•	
	BSP-4453	C	CVE-2021-46848 (libtasn1)	•	•	•	
	BSP-4432	C	CVE-2022-41741 (nginx)	•	•	•	
	BSP-4422	C	CVE-2022-3626 (tiff)	•	•	•	
	BSP-4421	C	CVE-2022-3599 (tiff)	•	•	•	
	BSP-4420	C	CVE-2022-3598 (tiff)	•	•	•	
	BSP-4419	C	CVE-2022-3597 (tiff)	•	•	•	
	BSP-4418	C	CVE-2022-3627 (tiff)	•	•	•	
	BSP-4417	C	CVE-2022-3566 (linux-imx-rt)	•	•	•	
	BSP-4416	C	CVE-2022-3567 (linux-imx-rt)	•	•	•	
	BSP-4415	C	CVE-2022-3594 (linux-imx-rt)	•	•	•	
	BSP-4412	C	CVE-2022-3570 (tiff)	•	•	•	
	BSP-4408	C	CVE-2022-3542 (linux-imx-rt)	•	•	•	
	BSP-4390	C	CVE-2012-6687 (fcgi)	•	•	•	
	BSP-4389	C	CVE-2022-3435 (linux-imx-rt)	•	•	•	
	BSP-4386	C	CVE-2022-42703 (linux-imx-rt)	•	•	•	
	BSP-4385	C	CVE-2022-42721 (linux-imx-rt)	•	•	•	
	BSP-4384	C	CVE-2022-42722 (linux-imx-rt)	•	•	•	
	BSP-4375	C	CVE-2021-28691 (linux-imx-rt)	•	•	•	
	BSP-4369	C	CVE-2022-0847 (linux-imx-rt)	•	•	•	
	BSP-4365	C	CVE-2022-0185 (linux-imx-rt)	•	•	•	
	BSP-4350	C	CVE-2021-3782 (wayland)	•	•	•	
	BSP-4348	C	CVE-2022-35252 (curl)	•	•	•	
	BSP-4342	C	CVE-2022-1475 (ffmpeg)	•	•	•	
	BSP-4341	C	CVE-2021-3566 (ffmpeg)	•	•	•	
	BSP-4338	C	CVE-2022-41218 (linux-ti)	•	•	•	
	BSP-4337	C	CVE-2020-20902 (ffmpeg)	•	•	•	
	BSP-4336	C	CVE-2021-38291 (ffmpeg)	•	•	•	
	BSP-4335	C	CVE-2021-38094 (ffmpeg)	•	•	•	
	BSP-4334	C	CVE-2021-38093 (ffmpeg)	•	•	•	
	BSP-4333	C	CVE-2021-38092 (ffmpeg)	•	•	•	
	BSP-4332	C	CVE-2021-38091 (ffmpeg)	•	•	•	
	BSP-4331	C	CVE-2021-38090 (ffmpeg)	•	•	•	
	BSP-4330	C	CVE-2020-20898 (ffmpeg)	•	•	•	
	BSP-4329	C	CVE-2020-20896 (ffmpeg)	•	•	•	
	BSP-4328	C	CVE-2020-20892 (ffmpeg)	•	•	•	

Version	Ticket ID	Type	Summary	UN60	UN65	UN78	Notes
	BSP-4328	C	CVE-2020-20892 (ffmpeg)	•	•	•	
	BSP-4327	C	CVE-2020-20891 (ffmpeg)	•	•	•	
	BSP-4249	C	CVE-2022-0168 (linux-imx-rt)	•	•	•	
	BSP-4196	C	CVE-2022-39188 (linux-imx-rt)	•	•	•	
	BSP-4193	C	CVE-2022-40307 (linux-imx-rt)	•	•	•	
	BSP-4180	C	CVE-2020-27820 (linux-imx-rt)	•	•	•	
	BSP-4165	C	CVE-2022-2663 (linux-imx-rt)	•	•	•	
	BSP-4135	C	CVE-2021-3759 (linux-imx-rt)	•	•	•	
	BSP-4059	C	CVE-2022-36879 (linux-imx-rt)	•	•	•	
	BSP-4035	C	CVE-2022-2078 (linux-imx-rt)	•	•	•	
	BSP-4025	C	CVE-2022-39190 (linux-imx-rt)	•	•	•	
	BSP-4022	C	CVE-2022-2380 (linux-imx-rt)	•	•	•	
	BSP-4016	C	C-2021-30470 (podofo)	•	•	•	
	BSP-3940	C	C-2021-30469 (podofo)	•	•	•	
	BSP-3916	C	C-2021-30471 (podofo)	•	•	•	
	BSP-3906	C	CVE-2020-36516 (linux-imx-rt)	•	•	•	
	BSP-3855	C	CVE-2021-4209 (gnutls)	•	•	•	
	BSP-3775	C	CVE-2021-44733 (linux-imx-rt)	•	•	•	
	BSP-3571	C	C-2021-30472 (podofo)	•	•	•	
	BSP-3545	C	CVE-2022-2977 (linux-imx-rt)	•	•	•	
	BSP-3426	C	CVE-2022-29824 (libxslt)	•	•	•	
	BSP-3420	C	CVE-2021-3999 (glibc)	•	•	•	
	BSP-3419	C	CVE-2019-11331 (ntp)	•	•	•	
	BSP-3418	C	CVE-2021-38593 (qtbase)	•	•	•	
	BSP-3414	C	CVE-2021-3672 (c-ares)	•	•	•	
	BSP-3412	C	CVE-2020-1730 (libssh)	•	•	•	
	BSP-3411	C	CVE-2019-14889 (libssh)	•	•	•	
	BSP-3410	C	CVE-2021-45951, CVE-2021-45952, CVE-2021-45953, CVE-2021-45954, CVE-2021-45955, CVE-2021-45956, CVE-2021-45957 (dnsmasq)	•	•	•	
	BSP-3408	C	CVE-2022-1920 (gststreamer1.0-plugins-good)	•	•	•	
	BSP-3406	C	CVE-2013-4235 (shadow)	•	•	•	
	BSP-3405	C	CVE-2016-3709 (libxml2)	•	•	•	
	BSP-3404	C	CVE-2021-3618 (nginx)	•	•	•	
	BSP-3403	C	CVE-2022-0934 (dnsmasq)	•	•	•	
	BSP-3401	C	CVE-2015-8981 CVE-2018-14320 (podofo)	•	•	•	
	BSP-3400	C	CVE-2022-1921, CVE-2022-1922, CVE-2022-1923, CVE-2022-1924, CVE-2022-1925, CVE-2022-2122 gststreamer1.0-plugins-good	•	•	•	
	BSP-3399	C	CVE-2022-2953 (libtiff)	•	•	•	

Version	Ticket ID	Type	Summary	UN60	UN65	UN78	Notes
	BSP-3398	C	CVE-2020-29260 (libvncserver)	•	•	•	
	BSP-3397	C	CVE-2021-4122 (cryptsetup)	•	•	•	
	BSP-3396	C	CVE-2022-35737 (sqlite3)	•	•	•	
	BSP-3395	C	CVE-2021-46828 (libtirpc)	•	•	•	
	BSP-3394	C	CVE-2022-29154 (rsync)	•	•	•	
	BSP-3393	C	CVE-2021-4209 (gnutls)	•	•	•	
	BSP-3391	C	CVE-2020-35538 (libjpeg-turbo)	•	•	•	
	BSP-3390	C	CVE-2022-2509 (gnutls)	•	•	•	
	BSP-3389	C	CVE-2021-46829 (gdk-pixbuf)	•	•	•	
	BSP-3387	C	CVE-2022-1271 (gzip)	•	•	•	
	BSP-3386	C	CVE-2022-37434 (zlib)	•	•	•	
	BSP-3375	C	CVE-2022-2867, CVE-2022-2868, CVE-2022-2869, CVE-2022-34526, CVE-2022-2056, CVE-2022-2057, CVE-2022-2058 (libtiff)	•	•	•	
	BSP-3263	C	CVE-2022-2068 (openssl)	•	•	•	
	BSP-3213	C	CVE-2022-28391 (busybox)	•	•	•	
	BSP-3212	C	CVE-2022-27404, CVE-2022-27405, CVE-2022-27406 (freetype)	•	•	•	
	BSP-3200	C	CVE-2022-1292 (openssl)	•	•	•	
	BSP-3143	C	CVE-2018-25032 (zlib)	•	•	•	
	BSP-3135	C	CVE-2022-23308 (libxml)	•	•	•	
	BSP-3133	C	CVE-2022-0547 (openvpn)	•	•	•	
	BSP-3132	C	CVE-2022-0778 (openssl)	•	•	•	
	BSP-3131	C	CVE-2022-0865, CVE-2022-0891, CVE-2022-0907, CVE-2022-0908, CVE-2022-0909, CVE-2022-0924 (libtiff)	•	•	•	
	BSP-3048	C	us01 us03 us04 ns01 kernel 4.14 CVE fixes #7	•	•	•	
	BSP-2772	C	CVE-2021-33574 (glibc)	•	•	•	
	BSP-2770	C	CVE-2021-23017 (nginx)	•	•	•	
	BSP-2726	C	CVE-2020-15078, CVE-2020-27569 (OpenVPN)	•	•	•	
	BSP-2718	C	CVE-2020-8252 (nodejs)	•	•	•	
	BSP-2717	C	CVE-2019-16275, CVE-2019-5061, CVE-2021-0326, CVE-2021-27803, CVE-2020-12695 (hostapd)	•	•	•	