TABLE I

24-HOUR BUG DETECTION FOR 10 RUNS OF THUNDERKALLER AND SYZKALLER. THE THIRD AND FOURTH COLUMNS SHOW THE MINIMUM TIME-TO-EXPOSURE (TTE) OF BUGS AMONG 10 RUNS. THE FIFTH AND SIXTH COLUMNS SHOW THE TOTAL NUMBER OF TRIGGERED RUNS. THE LAST COLUMN SHOWS WHETHER SYZBOT HAS ALREADY DETECTED THIS BUG. (BUGS UNIQUELY FOUND BY THUNDERKALLER ARE OMITTED.)

Crash Type	Function	Min. TTE		Crash Discovered		
		Th*	Syz*	Th*	Syz*	Syzbot
Use-after-free	fw_load_sysfs_fallback	**00h48m**	06h58m	10	3	✓
Use-after-free	kill_pending_fw_fallback_reqs	**00h50m**	07h14m	10	4	✓
Use-after-free	fb_mode_is_equal	**02h00m**	03h03m	10	10	✓
Use-after-free	ntfs_test_inode	**14h16m**	21h04m	3	2	✓
Use-after-free	lock_sock_nested	**01h30m**	22h25m	3	2	✓
Use-after-free	diFree	**04h50m**	06h10m	1	1	✓
Out-of-bounds	soft_cursor	**01h14m**	(N/A)	2	0	✓
Out-of-bounds	leaf_paste_entries	**10h04m**	20h12m	10	7	✓
Inconsistent lock state	waiting for DEV to become free	**04h00m**	04h31m	8	5	✓
Protection fault	cgroup_file_write	**02h42m**	13h13m	5	4	✓
Page fault	imageblit	08h46m	**06h34m**	5	8	✓
Warning	account_page_dirtied	**00h14m**	06h47m	10	10	✓
Warning	f2fs_is_valid_blkaddr	04h12m	**03h38m**	8	10	✓
Warning	kthread_is_per_cpu	**07h48m**	15h38m	7	4	✓
Warning	sta_info_insert_rcu	**04h04m**	07h02m	10	9	✓
Warning	floppy_queue_rq	**08h36m**	14h26m	6	4	✓
Warning	pwq_unbound_release_workfn	**06h02m**	18h21m	9	8	✓
Warning	submit_bio_checks	**00h43m**	05h21m	6	3	✓
Warning	xfs_destroy_mount_workqueues	**03h21m**	05h55m	1	2	✓
Warning	j1939_sk_queue_activate_next	18h21m	**12h13m**	1	1	✓
Warning	send_hsr_supervision_frame	**00h22m**	01h06m	10	2	✓
Warning	hci_conn_timeout	**01h20m**	06h22m	10	3	✓
Warning	ieee80211_bss_info_change-_notify	**01h55m**	06h19m	10	1	✓
Warning	close_fs_devices	04h22m	**03h16m**	10	10	✓
Warning	netdev_run_todo	**08h01m**	08h59m	5	2	✓
Warning	nbd_dev_add	(N/A)	01h46m	0	1	✓
Task hung	hub_port_init	**04h09m**	19h44m	8	1	✓
Task hung	__unmap_and_move	**00h37m**	07h55m	7	3	✓
Task hung	blkdev_put	**03h36m**	12h55m	7	2	✓
Task hung	p9_fd_close	**00h28m**	11h40m	8	1	✓
Task hung	sync_inodes_sb	**01h18m**	02h50m	8	9	✓
Task hung	gfs2_make_fs_ro	**13h16m**	17h51m	1	2	✓
Task hung	do_proc_bulk	**00h44m**	07h55m	8	2	✓
Task hung	io_uring_cancel_task_requests	**02h32m**	09h13m	6	1	✓
Deadlock	console_lock_spinning_enable	**04h05m**	07h16m	10	10	✓
Deadlock	console_trylock_spinning	**04h06m**	19h18m	8	3	✓
Kernel bug	do_journal_end	**00h34m**	04h05m	2	1	✓
Kernel bug	f2fs_new_node_page	(N/A)	22h13m	0	1	✗
Kernel bug	gfs2_glock_nq	**03h51m**	06h07m	6	1	✓

Syz*: Syzkaller; Th*: Thunderkaller.