Table 2: 24-hour crash detection for 10 runs of Thunderkaller and Syzkaller. The third and fourth columns show the minimum time-to-exposure (TTE) of the crash among 10 runs. The fifth and sixth columns show the total number of triggered runs and triggered times (#triggered runs / #triggered times). The last column shows whether Syzbot has already detected the unique crash. (Crashes uniquely found by Thunderkaller are omitted.)

Crash Type	Function	Time Spend		Crash Discovered		
		Th*	Syz*	Th*	Syz*	Syzbot
Use-after-free	fw_load_sysfs_fallback	**00h48m**	06h58m	10/30	3/8	✓
Use-after-free	kill_pending_fw_fallback_reqs	**00h50m**	07h14m	10/33	4/11	✓
Use-after-free	fb_mode_is_equal	**02h00m**	03h03m	10/61	10/29	✓
Use-after-free	ntfs_test_inode	**14h16m**	21h04m	3/5	2/2	✓
Use-after-free	lock_sock_nested	**01h30m**	22h25m	3/3	2/2	✓
Use-after-free	diFree	**04h50m**	06h10m	1/1	1/1	✓
Out-of-bounds	soft_cursor	**01h14m**	03h58m	2/2	1/1	✓
Out-of-bounds	leaf_paste_entries	**10h04m**	20h12m	10/13	7/10	✓
Inconsistent lock state	waiting for DEV to become free	**04h00m**	04h31m	8/43	5/18	✓
Protection fault	cgroup_file_write	**02h42m**	13h13m	5/10	4/5	✓
Page fault	imageblit	08h46m	**06h34m**	5/13	8/20	✓
Warning	account_page_dirtied	**00h14m**	06h47m	10/113	10/78	✓
Warning	f2fs_is_valid_blkaddr	04h12m	**03h38m**	8/74	10/91	✓
Warning	kthread_is_per_cpu	**07h48m**	15h38m	7/25	4/10	✓
Warning	sta_info_insert_rcu	**04h04m**	07h02m	10/31	9/20	✓
Warning	floppy_queue_rq	**08h36m**	14h26m	6/11	4/7	✓
Warning	pwq_unbound_release_workfn	**06h02m**	18h21m	9/12	8/12	✓
Warning	submit_bio_checks	**00h43m**	05h21m	6/13	3/3	✓
Warning	xfs_destroy_mount_work-queues	**03h21m**	05h55m	1/1	2/3	✓
Warning	j1939_sk_queue_activate_next	18h21m	**12h13m**	1/1	1/1	✓
Warning	send_hsr_supervision_frame	**00h22m**	01h06m	10/20	2/3	✓
Warning	hci_conn_timeout	**01h20m**	06h22m	10/18	3/3	✓
Warning	ieee80211_bss_info_change_-notify	**01h55m**	06h19m	10/16	1/1	✓
Warning	close_fs_devices	04h22m	**03h16m**	10/55	10/62	✓
Warning	netdev_run_todo	**08h01m**	08h59m	5/5	2/2	✓
Warning	nbd_dev_add	(N/A)	01h46m	0/0	1/1	✓
Task hung	hub_port_init	**04h09m**	19h44m	8/10	1/1	✓
Task hung	__unmap_and_move	**00h37m**	07h55m	7/18	3/7	✓
Task hung	blkdev_put	**03h36m**	12h55m	7/13	2/3	✓
Task hung	p9_fd_close	**00h28m**	11h40m	8/10	1/1	✓
Task hung	sync_inodes_sb	**01h18m**	02h50m	8/20	9/13	✓
Task hung	gfs2_make_fs_ro	**13h16m**	17h51m	1/1	2/2	✓
Task hung	do_proc_bulk	**00h44m**	07h55m	8/10	2/3	✓
Task hung	io_uring_cancel_task_requests	**02h32m**	09h13m	6/8	1/1	✓
Deadlock	console_lock_spinning_enable	**04h05m**	07h16m	10/41	10/32	✓
Deadlock	console_trylock_spinning	**04h06m**	19h18m	8/16	3/7	✓
Kernel bug	do_journal_end	**00h34m**	04h05m	2/2	1/1	✓
Kernel bug	f2fs_new_node_page	(N/A)	22h13m	0/0	1/1	✗
Kernel bug	gfs2_glock_nq	**03h51m**	06h07m	6/11	1/1	✓

Syz*: Syzkaller; Th*: Thunderkaller.