Appendix

A. Bug List found by RDFuzz

TABLE III: Bugs Found by RDFuzz

Browser Version	Summary	Module	Rendering Stage	Type	Report ID	Status
Chromium-97.0.4689.0	Requested allocation size overflow	Skia	Paint	ASAN Detected	1301074	Confirmed
Chromium-97.0.4689.0	Rounded rect with negative left width	Blink	Layout	Assertion Bug	1301077	Fixed
Chromium-97.0.4689.0	Rounded rect with negative top width	Blink	Layout	Assertion Bug	1301158	Duplicated
Chromium-97.0.4689.0	Font without vertical baseline	Blink	Layout	Assertion Bug	1301159	WontFix
Chromium-97.0.4689.0	Max size less than layout unit	Blink	Layout	Assertion Bug	1301068	Confirmed
Chromium-97.0.4689.0	Max out size and content size not equal	Blink	Layout	Assertion Bug	1301076	Confirmed
Chromium-97.0.4689.0	Intrinsic size larger than border padding block sum	Blink	Layout	Assertion Bug	1301075	WontFix
Chromium-97.0.4689.0	Fit on one line failed	Blink	Layout	Assertion Bug	1301070	Confirmed
Chromium-97.0.4689.0	Rewind can not break after some element	Blink	Layout	Assertion Bug	1290675	Duplicated
Chromium-97.0.4689.0	count larger than max backing store	Blink	Other	Assertion Bug	1301073	WontFix
Chromium-97.0.4689.0	Bound not equal to edge	Blink	Paint	Assertion Bug	1301157	WontFix
Chromium-97.0.4689.0	PostLayoutScope not allowed	Blink	Layout	Assertion Bug	1301160	WontFix
Chromium-97.0.4689.0	Overlay overflow controls	Blink	Layout	Assertion Bug	1301161	WontFix
Chromium-104.0.5109.0	Bound quad not equal to edge$_{quad}$	Blink	Paint	Assertion Bug	1357961	Confirmed
Chromium-104.0.5109.0	Expansion bounds not contain rect	Blink	Paint	Assertion Bug	1355841	Confirmed
Chromium-104.0.5109.0	Child of node no need to reattach LayoutTree	Blink	Render Tree	Assertion Bug	1357982	Confirmed
Chromium-104.0.5109.0	Rect cannot conatin	Blink	Paint	Assertion Bug	1357624	Confirmed
Chromium-104.0.5109.0	Interval high not equal to container bottom	Blink	Layout	Assertion Bug	1357620	Confirmed
Chromium-104.0.5109.0	Local border box properties is empty	Blink	Layout	Assertion Bug	1357619	Confirmed
Chromium-104.0.5109.0	HashMap found no value for the given key	Blink	Other	Assertion Bug	1357534	Confirmed
Chromium-104.0.5109.0	Image left less than right	Blink	Render Tree	Assertion Bug	1357974	Confirmed
Chromium-104.0.5109.0	Pending images size not equel to size ordered set	Blink	Paint	Assertion Bug	1357968	Confirmed
Chromium-104.0.5109.0	Parent does not need layout	Blink	Layout	Assertion Bug	1357525	Confirmed
Chromium-104.0.5109.0	Layout witdh less than 0	Blink	Layout	Assertion Bug	1357615	Confirmed
Chromium-104.0.5109.0	Not RelPositioned	Blink	Layout	Assertion Bug	1355831	Duplicated
Chromium-104.0.5109.0	Main axis greater than layout unit	Blink	Layout	Assertion Bug	1356471	Duplicated
Chromium-104.0.5109.0	Total flex grow of current line less than 0	Blink	Layout	Assertion Bug	1357564	Duplicated
Chromium-104.0.5109.0	Content size less than layout unit	Blink	Layout	Assertion Bug	1357532	Duplicated
Chromium-104.0.5109.0	Preferred logical width less than layout unit	Blink	Layout	Assertion Bug	1357565	Confirmed
Chromium-104.0.5109.0	Definite height is not kUnknown	Blink	Layout	Assertion Bug	1357555	Confirmed
Chromium-104.0.5109.0	Parent cursor is null	Blink	Layout	Assertion Bug	1357986	Confirmed
Chromium-104.0.5109.0	Column sets is invalidated	Blink	Layout	Assertion Bug	1357614	Duplicated
Chromium-104.0.5109.0	Can not cast to LayoutNGTextCombine	Blink	Layout	Assertion Bug	1357577	Confirmed
Chromium-104.0.5109.0	Child Layout Blocked By Display Lock	Blink	Layout	Assertion Bug	1353672	Confirmed
Chromium-104.0.5109.0	Table body not start with first body	Blink	Layout	Assertion Bug	1357566	Confirmed
Chromium-104.0.5109.0	Layout value less than 0	Blink	Layout	Assertion Bug	1357499	Duplicated
Chromium-104.0.5109.0	Sticky position object count is 0	Blink	Render Tree	Assertion Bug	1357540	Confirmed
Chromium-104.0.5109.0	Value cannot cast to double	Blink	Other	Assertion Bug	1357585	Confirmed
Chromium-104.0.5109.0	Child with adjoining problem	Blink	Layout	Assertion Bug	1357985	Duplicated
Chromium-104.0.5109.0	Layout result not adjoining	Blink	Layout	Assertion Bug	1357987	Confirmed
Chromium-104.0.5109.0	Previous inflow position not empty	Blink	Layout	Assertion Bug	1357989	Confirmed
Chromium-104.0.5109.0	Container builder block offset is 0	Blink	Layout	Assertion Bug	1357976	Confirmed
Chromium-104.0.5109.0	Node is not a scroll container	Blink	Layout	Assertion Bug	1357952	Confirmed
Chromium-104.0.5109.0	Flex border box less than main axis border padding	Blink	Layout	Assertion Bug	1357597	Duplicated
Chromium-104.0.5109.0	Content size suggestion less than border padding	Blink	Layout	Assertion Bug	1357529	Confirmed
Chromium-104.0.5109.0	Grid size less than 0	Blink	Layout	Assertion Bug	1357547	Confirmed
Chromium-104.0.5109.0	Old block size not equal to the new	Blink	Layout	Assertion Bug	1357971	Confirmed
Chromium-104.0.5109.0	Space Writing Mode not equal to the style's	Blink	Layout	Assertion Bug	1357981	Confirmed
Chromium-104.0.5109.0	Inline size less than border padding Sum	Blink	Layout	Assertion Bug	1357527	Confirmed
Chromium-104.0.5109.0	Width to rewind less than 0	Blink	Layout	Assertion Bug	1357558	Confirmed
Chromium-104.0.5109.0	Item EndOffset after before	Blink	Layout	Assertion Bug	1356470	Duplicated
Chromium-104.0.5109.0	New item cannot break after old one	Blink	Layout	Assertion Bug	1357955	Confirmed
Chromium-104.0.5109.0	Style cannot auto wrap	Blink	Layout	Assertion Bug	1357963	Confirmed
Chromium-104.0.5109.0	Inline size greater than child	Blink	Layout	Assertion Bug	1357965	Confirmed
Chromium-104.0.5109.0	Container writing mode not equal to inline's	Blink	Layout	Assertion Bug	1357990	Confirmed
Chromium-104.0.5109.0	Hidden paint is not equal	Blink	Layout	Assertion Bug	1357616	Confirmed
Chromium-104.0.5109.0	Depends on percentage block size not equal	Blink	Layout	Assertion Bug	1357600	Confirmed
Chromium-104.0.5109.0	Padding not equal	Blink	Layout	Assertion Bug	1357579	Confirmed
Chromium-104.0.5109.0	Not all children are LineBox	Blink	Layout	Assertion Bug	1357973	Confirmed
Chromium-104.0.5109.0	Inline size before collapse greater than 1	Blink	Layout	Assertion Bug	1354128	Duplicated
Chromium-104.0.5109.0	Min size greater than max size	Blink	Layout	Assertion Bug	1357953	Confirmed
Chromium-104.0.5109.0	Preserves3D check failed	Blink	Paint	Assertion Bug	1356467	Confirmed
Chromium-104.0.5109.0	Raster contents scale is nan	Blink	Paint	Assertion Bug	1357551	Confirmed
Chromium-104.0.5109.0	Last geometry rect right not equal to current	Blink	Paint	Assertion Bug	1357979	Confirmed

TABLE IV: Bugs Found by RDFuzz- Continuation Table

Browser Version	Summary	Module	Rendering Stage	Type	Report ID	Status
Chromium-104.0.5109.0	Rect not contains skewport	Blink	Paint	Assertion Bug	1357537	Confirmed
Chromium-104.0.5109.0	Subtree has no update reason	Blink	Paint	Assertion Bug	1357530	Confirmed
Chromium-104.0.5109.0	Fragment id not equal	Blink	Paint	Assertion Bug	1357983	Confirmed
Chromium-104.0.5109.0	Node existense check failed	Blink	Render Tree	Assertion Bug	1357978	Confirmed
Chromium-104.0.5109.0	Dest id not descendant to current id	Blink	Render Tree	Assertion Bug	1357548	Confirmed
Chromium-104.0.5109.0	Scroll offset delta too big	Blink	Render Tree	Assertion Bug	1357580	Confirmed
Chromium-104.0.5109.0	Transform is not identitied	Blink	Paint	Assertion Bug	1357546	Confirmed
Chromium-104.0.5109.0	Invalid real effect	Blink	Paint	Assertion Bug	1357561	Confirmed
Chromium-104.0.5109.0	Constraints not cantain nearest sticky layer	Blink	Render Tree	Assertion Bug	1357627	Confirmed
Chromium-104.0.5109.0	Font writing mode is not null	Blink	Render Tree	Assertion Bug	1356469	Confirmed
Chromium-104.0.5109.0	Viewport unit flags is not null	Blink	Render Tree	Assertion Bug	1354932	Confirmed
Chromium-104.0.5109.0	Text run paint length less than from	Blink	Paint	Assertion Bug	1357552	Confirmed
Chromium-104.0.5109.0	Line midpoint state not equal	Blink	Layout	Assertion Bug	1357544	Confirmed
Chromium-104.0.5109.0	Transformation matrix is nan	Blink	Other	Assertion Bug	1357531	Confirmed
Chromium-104.0.5109.0	Row Qualifies As Significant check failed	Blink	Other	Assertion Bug	1357583	Confirmed
Chromium-104.0.5109.0	V8 process OOM	V8	Other	Assertion Bug	1353665	WontFix
WebKitGTK 2.36.0	Not all element need layout	WebCore	Layout	Assertion Bug	244599	Reported
WebKitGTK 2.36.0	Inner contains outer	WebCore	Layout	Assertion Bug	244469	Reported
WebKitGTK 2.36.0	Renderer of layout is not itself	WebCore	Layout	Assertion Bug	235572	Reported
WebKitGTK 2.36.0	Layout delta not Matches to oldLayoutDelta	WebCore	Layout	Assertion Bug	244466	Reported
WebKitGTK 2.36.0	Fragmented flow not in flow fragment	WebCore	Layout	Assertion Bug	235568	Reported
WebKitGTK 2.36.0	Outline bounds rect not equal to its container	WebCore	Layout	Assertion Bug	235567	Reported
WebKitGTK 2.36.0	Last word boundary is not the real last	WebCore	Layout	Assertion Bug	244464	Reported
WebKitGTK 2.36.0	NewRadii bottomLeft invalid	WebCore	Layout	Assertion Bug	237249	Reported
WebKitGTK 2.36.0	NewRadii topLeft invalid	WebCore	Layout	Assertion Bug	244470	Reported
WebKitGTK 2.36.0	NewRadii topRight invalid	WebCore	Layout	Assertion Bug	244583	Reported
WebKitGTK 2.36.0	NewRadii bottomRight invalid	WebCore	Layout	Assertion Bug	244592	Reported
WebKitGTK 2.36.0	Ellipsis Box exists	WebCore	Layout	Assertion Bug	244465	Reported
WebKitGTK 2.36.0	Index invalid	WebCore	Layout	Assertion Bug	244595	Reported
WebKitGTK 2.36.0	Node cannot calculated	WebCore	Layout	Assertion Bug	244598	Reported
WebKitGTK 2.36.0	Fragments are invalidated	WebCore	Layout	Assertion Bug	244463	Reported
WebKitGTK 2.36.0	ScrolldDimensions are dirty	WebCore	Layout	Assertion Bug	244589	Reported
WebKitGTK 2.36.0	Visible content status is dirty	WebCore	Layout	Assertion Bug	244581	Reported
WebKitGTK 2.36.0	Mode contains fixed node	WebCore	Layout	Assertion Bug	244596	Reported
WebKitGTK 2.36.0	Target source invalid	WebCore	Layout	Assertion Bug	244597	Reported
WebKitGTK 2.36.0	Page count is non-utility	WebCore	Layout	Assertion Bug	244586	Reported
WebKitGTK 2.36.0	RendererMappedResult not equal old result	WebCore	Layout	Assertion Bug	244467	Reported
WebKitGTK 2.36.0	Container block cannot have box info in fragment()	WebCore	Layout	Assertion Bug	244587	Reported
WebKitGTK 2.36.0	Content size is 0	WebCore	Layout	Assertion Bug	237250	Reported
WebKitGTK 2.36.0	Found ancestor in node	WebCore	Layout	Assertion Bug	244588	Reported
WebKitGTK 2.36.0	Node is placed	WebCore	Layout	Assertion Bug	244580	Reported
WebKitGTK 2.36.0	Line White space Collapsing State not equel	WebCore	Layout	Assertion Bug	244584	Reported
WebKitGTK 2.36.0	Accumulated Offset not Saturated	WebCore	Layout	Assertion Bug	244462	Reported
WebKitGTK 2.36.0	MeasuredWidth less than 0	WebCore	Layout	Assertion Bug	244582	Reported
WebKitGTK 2.36.0	Logical position not intersect	WebCore	Layout	Assertion Bug	244591	Reported
WebKitGTK 2.36.0	Element position invalid	WebCore	Layout	Assertion Bug	235569	Reported
WebKitGTK 2.36.0	Total Flex Grow is negative	WebCore	Layout	Assertion Bug	244590	Reported
WebKitGTK 2.36.0	Renderers With Outline Count is 0	WebCore	Layout	Assertion Bug	244585	Reported
FireFox Nightly 94.0.1	Stack Overflow	libxul	Layout	ASAN Detected	1738464	Reported
FireFox Nightly 101.0a1	Flex Container Frame invalid	layout	Layout	Assertion Bug	1787695	Reported
FireFox Nightly 101.0a1	WM Is not Orthogonal To target	layout	Layout	Assertion Bug	1787693	Reported
FireFox Nightly 101.0a1	Multiplication of infinity by zero	layout	Other	Assertion Bug	1757319	Reported
FireFox Nightly 101.0a1	A child is also an ancestor	layout	Layout	Assertion Bug	1787690	Reported
FireFox Nightly 101.0a1	The bbox is about to go bad	layout	Layout	Assertion Bug	1788189	Reported
FireFox Nightly 101.0a1	Invalid event delivery	layout	Layout	Assertion Bug	1757323	Duplicated
FireFox Nightly 101.0a1	Unconstrained block-size	layout	Layout	Assertion Bug	1788184	Reported
FireFox Nightly 101.0a1	Invalid end line	layout	Layout	Assertion Bug	1787697	Reported
FireFox Nightly 101.0a1	Unprocessed justification width	layout	Layout	Assertion Bug	1787689	Reported
FireFox Nightly 101.0a1	Line break inside ruby box not suppressed	layout	Layout	Assertion Bug	1788185	Confirmed
FireFox Nightly 101.0a1	Item should have finite clip with respect to aASR	layout	Layout	Assertion Bug	1757326	Duplicated
FireFox Nightly 101.0a1	Out Of Flow Frame not equal	layout	Layout	Assertion Bug	1788194	Reported
FireFox Nightly 101.0a1	Value n2 less than -epsilon	layout	Other	Assertion Bug	1787694	Reported
FireFox Nightly 101.0a1	Unexpected containing block size	layout	Layout	Assertion Bug	1788184	Reported
FireFox Nightly 101.0a1	Render border is negative	layout	Layout	Assertion Bug	1788192	Confirmed