Alpine Linux - Bug #7422

[3.6] webkit2gtk: Several vulnerabilities (Various CVEs)

06/13/2017 08:08 AM - Alicha CH

Status:	Closed	**Start date:**	06/13/2017
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	100%
Category:	Security	**Estimated time:**	0.00 hour
Target version:	3.6.2		
Affected versions:		**Security IDs:**	

Description

CVE-2016-9643:The regex code in WebKit allows remote attackers to cause a denial of service (memory consumption) as demonstrated in a large number of
($ (open parenthesis and dollar) followed by {-2,16} and a large number of +) (plus close parenthesis).

Versions affected: WebKitGTK+ before 2.14.6

CVE-2017-2367: This issue allows remote attackers to bypass the Same Origin Policy and obtain sensitive information via a crafted web site.

Versions affected: WebKitGTK+ before 2.14.6.

CVE-2017-2377: This issue involves the “WebKit Web Inspector” component. It allows attackers to cause a denial of service (memory corruption and application crash)
by leveraging a window-close action during a debugger-pause state.

Versions affected: WebKitGTK+ before 2.14.6.

CVE-2017-2392: This issue allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted app.

Versions affected: WebKitGTK+ before 2.14.6.

CVE-2017-2394: This issue allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.

Versions affected: WebKitGTK+ before 2.14.6.

CVE-2017-2415: This issue allows remote attackers to execute arbitrary code by leveraging an unspecified “type confusion.”.

Versions affected: WebKitGTK+ before 2.14.6.

CVE-2017-2419: This issue allows remote attackers to bypass a Content Security Policy protection mechanism via unspecified vectors.

Versions affected: WebKitGTK+ before 2.14.6.

CVE-2017-2442: This issue involves the “WebKit JavaScript Bindings” component. It allows remote attackers to bypass the Same Origin Policy and
obtain sensitive information via a crafted web site.

Versions affected: WebKitGTK+ before 2.14.6.

CVE-2017-2446: This issue allows remote attackers to execute arbitrary code via a crafted web site that leverages the mishandling of strict mode functions.

Versions affected: WebKitGTK+ before 2.14.6.

CVE-2017-2454: This issue allows allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.

Versions affected: WebKitGTK+ before 2.14.6.

CVE-2017-2459: This issue allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.

Versions affected: WebKitGTK+ before 2.14.6.

CVE-2017-2460: This issue allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.

Versions affected: WebKitGTK+ before 2.14.6.

CVE-2017-2465: This issue allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.

Versions affected: WebKitGTK+ before 2.14.6.

CVE-2017-2466: This issue allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.

Versions affected: WebKitGTK+ before 2.14.6.

CVE-2017-2468: This issue allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.

Versions affected: WebKitGTK+ before 2.14.6.

CVE-2017-2470: This issue allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.

Versions affected: WebKitGTK+ before 2.14.6.

CVE-2017-2471: A use-after-free vulnerability allows remote attackers to execute arbitrary code via a crafted web site.

Versions affected: WebKitGTK+ before 2.14.6.

CVE-2017-2475: This issue allows remote attackers to conduct Universal XSS (UXSS) attacks via crafted use of frames on a web site.

Versions affected: WebKitGTK+ before 2.14.6.

CVE-2017-2476: This issue allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.

Versions affected: WebKitGTK+ before 2.14.6.

CVE-2017-2481: This issue allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.

Versions affected: WebKitGTK+ before 2.14.6.

Reference:

https://webkitgtk.org/security/WSA-2017-0003.html

Associated revisions

Revision 52d9e7b1 - 06/14/2017 07:56 AM - Natanael Copa

community/webkit2gtk: upgrade to 2.16.3

and enable on ppc64le and aarch64

CVE-2016-9642, CVE-2016-9643, CVE-2017-2364, CVE-2017-2367,
CVE-2017-2376, CVE-2017-2377, CVE-2017-2386, CVE-2017-2392,
CVE-2017-2394, CVE-2017-2395, CVE-2017-2396, CVE-2017-2405,
CVE-2017-2415, CVE-2017-2419, CVE-2017-2433, CVE-2017-2442,
CVE-2017-2445, CVE-2017-2446, CVE-2017-2447, CVE-2017-2454,
CVE-2017-2455, CVE-2017-2457, CVE-2017-2459, CVE-2017-2460,
CVE-2017-2464, CVE-2017-2465, CVE-2017-2466, CVE-2017-2468,
CVE-2017-2469, CVE-2017-2470, CVE-2017-2471, CVE-2017-2475,

CVE-2017-2476, CVE-2017-2481

CVE-2017-2496, CVE-2017-2504, CVE-2017-2505, CVE-2017-2506,
CVE-2017-2508, CVE-2017-2510, CVE-2017-2514, CVE-2017-2515,
CVE-2017-2521, CVE-2017-2525, CVE-2017-2526, CVE-2017-2528,
CVE-2017-2530, CVE-2017-2531, CVE-2017-2536, CVE-2017-2539,
CVE-2017-2544, CVE-2017-2547, CVE-2017-2549, CVE-2017-6980,
CVE-2017-6984.

fixes #7422

History

#1 - 06/14/2017 08:34 AM - Natanael Copa

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset alpine:52d9e7b149a47445bc334c456fbc736550584b66.

#2 - 06/14/2017 05:22 PM - Alicha CH

- Project changed from Alpine Security to Alpine Linux

- Category set to Security

- Status changed from Resolved to Closed