Alpine Linux - Bug #6888

Bug # 6886 (Closed): webkit2gtk: Several vulnerabilities (CVE-2017-2350, CVE-2017-2354, CVE-2017-2355, CVE-2017-2356, CVE-2017-2362, CVE-2017-2363, CVE-2017-2364, CVE-2017-2365, CVE-2017-2366, CVE-2017-2369, CVE-2017-2371, CVE-2017-2373)

[3.5] webkit2gtk: Several vulnerabilities (CVE-2017-2350, CVE-2017-2354, CVE-2017-2355, CVE-2017-2356, CVE-2017-2362, CVE-2017-2363, CVE-2017-2364, CVE-2017-2365, CVE-2017-2366, CVE-2017-2369, CVE-2017-2371, CVE-2017-2373)

02/17/2017 11:59 AM - Alicha CH

Status:	Closed	**Start date:**	02/17/2017
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	100%
Category:	Security	**Estimated time:**	0.00 hour
Target version:	3.5.2		
Affected versions:		**Security IDs:**	

Description

CVE-2017-2350

Versions affected: WebKitGTK+ before 2.14.4.
Impact: Processing maliciously crafted web content may exfiltrate data cross-origin.
Description: A prototype access issue was addressed through improved exception handling.

CVE-2017-2354

Versions affected: WebKitGTK+ before 2.14.4.
Impact: Processing maliciously crafted web content may lead to arbitrary code execution.
Description: Multiple memory corruption issues were addressed through improved memory handling.

CVE-2017-2355

Versions affected: WebKitGTK+ before 2.14.4.
Impact: Processing maliciously crafted web content may lead to arbitrary code execution.
Description: A memory initialization issue was addressed through improved memory handling.

CVE-2017-2356

Versions affected: WebKitGTK+ before 2.14.4.
Impact: Processing maliciously crafted web content may lead to arbitrary code execution.
Description: Multiple memory corruption issues were addressed through improved input validation.

CVE-2017-2362

Versions affected: WebKitGTK+ before 2.14.4.
Impact: Processing maliciously crafted web content may lead to arbitrary code execution.
Description: Multiple memory corruption issues were addressed through improved memory handling.

CVE-2017-2363

Versions affected: WebKitGTK+ before 2.14.4.
Impact: Processing maliciously crafted web content may exfiltrate data cross-origin.
Description: Multiple validation issues existed in the handling of page loading.
This issue was addressed through improved logic.

CVE-2017-2364

Versions affected: WebKitGTK+ before 2.14.4.
Impact: Processing maliciously crafted web content may exfiltrate data cross-origin.
Description: Multiple validation issues existed in the handling of page loading.
This issue was addressed through improved logic.

CVE-2017-2365

Versions affected: WebKitGTK+ before 2.14.4.
Impact: Processing maliciously crafted web content may exfiltrate data cross-origin.
Description: A validation issue existed in variable handling.
This issue was addressed through improved validation.

CVE-2017-2366

Versions affected: WebKitGTK+ before 2.14.4.
Impact: Processing maliciously crafted web content may lead to arbitrary code execution.
Description: Multiple memory corruption issues were addressed through improved input validation.

CVE-2017-2369

Versions affected: WebKitGTK+ before 2.14.4.
Impact: Processing maliciously crafted web content may lead to arbitrary code execution.
Description: Multiple memory corruption issues were addressed through improved input validation.

CVE-2017-2371

Versions affected: WebKitGTK+ before 2.14.4.
Impact: A malicious website can open popups.
Description: An issue existed in the handling of blocking popups.
This was addressed through improved input validation.

CVE-2017-2373

Versions affected: WebKitGTK+ before 2.14.4.
Impact: Processing maliciously crafted web content may lead to arbitrary code execution.
Description: Multiple memory corruption issues were addressed through improved memory handling.

Reference:

https://webkitgtk.org/security/WSA-2017-0002.html

Associated revisions

Revision 9eedb146 - 02/22/2017 11:20 AM - Sergei Lukin

community/webkit2gtk: security upgrade to 2.14.5 - fixes #6888

CVE-2017-2350
CVE-2017-2354
CVE-2017-2355
CVE-2017-2356
CVE-2017-2362
CVE-2017-2363
CVE-2017-2364
CVE-2017-2365
CVE-2017-2366
CVE-2017-2369
CVE-2017-2371
CVE-2017-2373

History

#1 - 02/22/2017 11:20 AM - Sergei Lukin

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset alpine:9eedb1462483dddad2de55715f16558844a078c5.

#2 - 02/23/2017 09:08 AM - Alicha CH

- Category set to Security

- Status changed from Resolved to Closed