Alpine Linux - Bug #9453

Bug # 9451 (Closed): webkit2gtk: Multiple vulnerabilities (CVE-2018-4246, CVE-2018-4261, CVE-2018-4262, CVE-2018-4263, CVE-2018-4264, CVE-2018-4265, CVE-2018-4266, CVE-2018-4267, CVE-2018-4270, CVE-2018-4272, CVE-2018-4273, CVE-2018-4278, CVE-2018-4284, CVE-2018-12911)

[3.8] webkit2gtk: Multiple vulnerabilities (CVE-2018-4246, CVE-2018-4261, CVE-2018-4262, CVE-2018-4263, CVE-2018-4264, CVE-2018-4265, CVE-2018-4266, CVE-2018-4267, CVE-2018-4270, CVE-2018-4272, CVE-2018-4273, CVE-2018-4278, CVE-2018-4284, CVE-2018-12911)

09/21/2018 10:37 AM - Alicha CH

Status:	Closed	**Start date:**	09/21/2018
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	100%
Category:	Security	**Estimated time:**	0.00 hour
Target version:	3.8.2		
Affected versions:		**Security IDs:**	

Description

CVE-2018-4246

Processing maliciously crafted web content may lead to arbitrary code execution.
A type confusion issue was addressed with improved memory handling.
Versions affected: WebKitGTK+ before 2.20.4

CVE-2018-4261

Processing maliciously crafted web content may lead to arbitrary code execution.
A memory corruption issue was addressed with improved memory handling.
Versions affected: WebKitGTK+ before 2.20.4

CVE-2018-4262

Processing maliciously crafted web content may lead to arbitrary code execution.
A memory corruption issue was addressed with improved memory handling.
Versions affected: WebKitGTK+ before 2.20.4

CVE-2018-4263

Processing maliciously crafted web content may lead to arbitrary code execution.
A memory corruption issue was addressed with improved memory handling.
Versions affected: WebKitGTK+ before 2.20.4

CVE-2018-4264

Processing maliciously crafted web content may lead to arbitrary code execution.
A memory corruption issue was addressed with improved memory handling.
Versions affected: WebKitGTK+ before 2.20.4

CVE-2018-4265

Processing maliciously crafted web content may lead to arbitrary code execution.
A memory corruption issue was addressed with improved memory handling.
Versions affected: WebKitGTK+ before 2.20.4

CVE-2018-4266

A malicious website may be able to cause a denial of service.
A race condition was addressed with additional validation.
Versions affected: WebKitGTK+ before 2.20.4 and WPE WebKit before 2.20.2.

CVE-2018-4267

Processing maliciously crafted web content may lead to arbitrary code execution.

A memory corruption issue was addressed with improved memory handling.
Versions affected: WebKitGTK+ before 2.20.4

CVE-2018-4270

Processing maliciously crafted web content may lead to an unexpected application crash.
A memory corruption issue was addressed with improved memory handling.
Versions affected: WebKitGTK+ before 2.20.4

CVE-2018-4272

Processing maliciously crafted web content may lead to arbitrary code execution.
A memory corruption issue was addressed with improved memory handling.
Versions affected: WebKitGTK+ before 2.20.4

CVE-2018-4273

Processing maliciously crafted web content may lead to an unexpected application crash.
A memory corruption issue was addressed with improved input validation.
Versions affected: WebKitGTK+ before 2.20.4

CVE-2018-4278

A malicious website may exfiltrate audio data cross-origin. Sound fetched through audio elements may be exfiltrated cross-origin. This issue was addressed with improved audio taint tracking.
Versions affected: WebKitGTK+ before 2.20.4

CVE-2018-4284

Processing maliciously crafted web content may lead to arbitrary code execution.
A type confusion issue was addressed with improved memory handling
Versions affected: WebKitGTK+ before 2.20.4
.
CVE-2018-12911

Processing maliciously crafted web content may lead to arbitrary code execution.
A buffer overflow issue was addressed with improved memory handling.
Versions affected: WebKitGTK+ before 2.20.4

Reference:

https://webkitgtk.org/security/WSA-2018-0006.html

Associated revisions

Revision 0af1cbfd - 09/27/2018 08:22 AM - Natanael Copa

community/webkit2gtk: security upgrade to 2.20.4

CVE-2018-4246, CVE-2018-4261, CVE-2018-4262, CVE-2018-4263,
CVE-2018-4264, CVE-2018-4265, CVE-2018-4266, CVE-2018-4267,
CVE-2018-4270, CVE-2018-4272, CVE-2018-4273, CVE-2018-4278,
CVE-2018-4284, CVE-2018-12911

fixes #9453

History

#1 - 09/27/2018 08:22 AM - Natanael Copa

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset alpine:0af1cbfdb6065fca513ef4d282a2c794faba6c18.

#2 - 10/02/2018 08:15 AM - Alicha CH

- Project changed from Alpine Security to Alpine Linux

- Category set to Security

- Status changed from Resolved to Closed

- Security IDs deleted (CVE-2018-4246, CVE-2018-4261, CVE-2018-4262, CVE-2018-4263, CVE-2018-4264, CVE-2018-4265, CVE-2018-4266, CVE-2018-4267, CVE-2018-4270, CVE-2018-4272, CVE-2018-4273, CVE-2018-4278, CVE-2018-4284, CVE-2018-12911)