Instituto
de Ciencias
Tecnológicas

INFORME DE VULNERABILIDADES

Fecha de Revisión: 22-05-2021

Autores: Estudiantes Instituto CIISA

Tabla de Contenido

1. Acuerdo de confidencialidad del documento.

1.1 Declaración de confidencialidad.

Toda la información contenida en este documento se proporciona con la confianza de que el único propósito es describir y evidenciar hallazgos en pruebas de seguridad y no se utilizará para ningún otro propósito, y no podrá ser publicado o divulgado en su totalidad o en parte, a cualquier otra persona o empresa sin el permiso previo de cliente por escrito. Estas obligaciones no se aplicarán a la información que se publica o ya se conoce legítimamente de otra fuente del cliente.

2. Descripción de las pruebas.

Para la revisión de vulnerabilidades se ejecutaron las siguientes pruebas

2.1 SAST.

Herramienta a utilizar: SonarQube.
Descripccion:
El análisis consiste en examinar el código fuente para detectar y reportar las debilidades que pueden conducir a vulnerabilidades de seguridad. La herramienta analiza el código fuente detectando vulnerabilidades de seguridad tales como “SQL Injection”, “Log Injection” o “X-site scripting” y otras vulnerabilidades que puedan estar presentes. El análisis incluye la verificación de cumplimiento de estándares de desarrollo y reglas de diseño.

2.2 IaC Security.

Herramienta a utilizar: Trivy.
Descripción:
El análisis consiste en revisar la imagen de contenedores Dockers para encontrar vulnerabilidades frecuentes en los servidores, este contendor asimila la infraestructura física de las dependencias del cliente por lo que las vulnerabilidades serán referenciales.

2.3 Vulnerability Checks.

Herramienta a utilizar: Rapidscan.
Descripción:
El análisis consiste en la detección de vulnerabilidades presentes en los servidores, este análisis contempla lo siguiente puntos acordados:

- Identificar presencia de DNS/HTTP Load Balancers & Web Application Firewalls.
- Verificaciones para Joomla, WordPress and Drupal
- Vulnerabilidades relacionadas con SSL (HEARTBLEED, FREAK, POODLE, CCS Injection, OGJAM, OCSP Stapling).
- Puertos comúnmente abiertos.
- Transferencias de zona DNS utilizando múltiples herramientas (Fierce, DNSWalk, DNSRecon, DNSEnum).
- Fuerza bruta de subdominios (DNSMap, amass, nikto)
- Abrir directorio / archivo de fuerza bruta.
- Banners superficiales XSS, SQLi y BSQLi.
- Ataque DoS de Slow-Loris, LFI (inclusión de archivos locales), RFI (Remote File Inclusion) & RCE (Remote Code Execution).

3. Historial de Revisiones al documento.

Número de revisión	Fecha de Revisión	Resumen de cambios
1.0	22-05-2021	Creación del documento

4. Datos del proyecto.

Nombre de proyecto	IADSO_CIISA_IECS_REPO_TEST
Repositorio	https://github.com/Vicentezapata/IADSO_CIISA_IECS_REPO_TEST.git
Categoría	WEBPAGE
Tipo de repositorio	Publico

5. Hallazgos.

5.1 Detalle de Hallazgos.

5.1.1 SonarQube.

SonarQube	
Severidad	**Cantidad**
Bloqueantes	5
Críticas	42
Importantes	413
Menores	69
Información	15

Detalle de vulnerabilidades de tipo: Bloqueantes

1. Componente: JavaScript/contact_me.js
   - Linea: 20
   - Acciones: Add the "let", "const" or "var" keyword to this declaration of "$this" to make it explicit.

2. Componente: JavaScript/dic_cursos.js
   - Linea: 96
   - Acciones: Add the "let", "const" or "var" keyword to this declaration of "out" to make it explicit.

3. Componente: JavaScript/dic_cursos.js
   - Linea: 97
   - Acciones: Add the "let", "const" or "var" keyword to this declaration of "i" to make it explicit.

4. Componente: JavaScript/dic_cursos.js
   - Linea: 154
   - Acciones: Add the "let", "const" or "var" keyword to this declaration of "cont" to make it explicit.

5. Componente: JavaScript/dic_cursos.js
   - Linea: 162

- Acciones: Add the "let", "const" or "var" keyword to this declaration of "req" to make it explicit.

Detalle de vulnerabilidades de tipo: Criticas

1. Componente: JavaScript/fb_sdk.js
   - Linea: 22
   - Acciones: Refactor this function to reduce its Cognitive Complexity from 17 to the 15 allowed.

2. Componente: JavaScript/jqBootstrapValidation.js
   - Linea: 32
   - Acciones: Refactor this function to reduce its Cognitive Complexity from 222 to the 15 allowed.

3. Componente: gym/controlador.php
   - Linea: 4
   - Acciones: Add a "case default" clause to this "switch" statement.

4. Componente: gym/controlador.php
   - Linea: 34
   - Acciones: Define a constant instead of duplicating this literal "<META HTTP-EQUIV="REFRESH" CONTENT="2;URL=index.php"> " 3 times.

5. Componente: gym/controlador.php
   - Linea: 139
   - Acciones: Define a constant instead of duplicating this literal "<META HTTP-EQUIV="REFRESH" CONTENT="2;URL=evaluacion.php"> " 3 times.

6. Componente: gym/logout.php
   - Linea: 24
   - Acciones: Define a constant instead of duplicating this literal "<META HTTP-EQUIV="REFRESH" CONTENT="2;URL=index.php"> " 3 times.

7. Componente: gym/visualizador.php
   - Linea: 177
   - Acciones: Define a constant instead of duplicating this literal "</td>" 5 times.

8. Componente: mail/contact_me.php
   - Linea: 20
   - Acciones: Add curly braces around the nested statement(s).

9. Componente: vendor/bootstrap/js/bootstrap.bundle.js
   - Linea: 10
   - Acciones: Refactor this function to reduce its Cognitive Complexity from 2047 to the 15 allowed.

10. Componente: vendor/bootstrap/js/bootstrap.bundle.js
    - Linea: 3736
    - Acciones: Unexpected empty method 'onCreate'.

11. Componente: vendor/bootstrap/js/bootstrap.bundle.js
    - Linea: 3746
    - Acciones: Unexpected empty method 'onUpdate'.

12. Componente: vendor/bootstrap/js/bootstrap.bundle.js
    - Linea: 3928
    - Acciones: This function expects 1 argument, but 2 were provided.

13. Componente: vendor/bootstrap/js/bootstrap.bundle.js
    - Linea: 4988
    - Acciones: This function expects 1 argument, but 2 were provided.

14. Componente: vendor/bootstrap/js/bootstrap.js
    - Linea: 10
    - Acciones: Refactor this function to reduce its Cognitive Complexity from 1521 to the 15 allowed.

15. Componente: vendor/bootstrap/js/bootstrap.js
    - Linea: 1411
    - Acciones: This function expects 1 argument, but 2 were provided.

16. Componente: vendor/bootstrap/js/bootstrap.js
    - Linea: 2471
    - Acciones: This function expects 1 argument, but 2 were provided.

17. Componente: vendor/jquery/jquery.js
    - Linea: 40
    - Acciones: Refactor this function to reduce its Cognitive Complexity from 24451 to the 15 allowed.

18. Componente: vendor/jquery/jquery.js
    - Linea: 308
    - Acciones: Unexpected empty method 'noop'.

19. Componente: vendor/jquery/jquery.js
    - Linea: 2127
    - Acciones: Unexpected empty function 'setFilters'.

20. Componente: vendor/jquery/jquery.js
    - Linea: 2442
    - Acciones: Remove this assignment of "i".

21. Componente: vendor/jquery/jquery.js
    - Linea: 3263
    - Acciones: This loop's stop condition tests "queue.length, queue" but the incrementer updates "firingIndex".

22. Componente: vendor/jquery/jquery.js
    - Linea: 3265
    - Acciones: Remove this assignment of "firingIndex".

23. Componente: vendor/jquery/jquery.js
    - Linea: 3272
    - Acciones: Remove this assignment of "firingIndex".

24. Componente: vendor/jquery/jquery.js
    - Linea: 7014
    - Acciones: Remove this assignment of "prop".

25. Componente: vendor/jquery/jquery.js
    - Linea: 7057
    - Acciones: Remove this assignment of "index".

26. Componente: vendor/jquery/jquery.js
    - Linea: 7437
    - Acciones: Remove this assignment of "i".

27. Componente: vendor/jquery/jquery.slim.js
    - Linea: 40
    - Acciones: Refactor this function to reduce its Cognitive Complexity from 18456 to the 15 allowed.

28. Componente: vendor/jquery/jquery.slim.js
    - Linea: 308
    - Acciones: Unexpected empty method 'noop'.

29. Componente: vendor/jquery/jquery.slim.js
    - Linea: 2127
    - Acciones: Unexpected empty function 'setFilters'.

30. Componente: vendor/jquery/jquery.slim.js
    - Linea: 2442
    - Acciones: Remove this assignment of "i".

31. Componente: vendor/jquery/jquery.slim.js
    - Linea: 3263
    - Acciones: This loop's stop condition tests "queue.length, queue" but the incrementer updates "firingIndex".

32. Componente: vendor/jquery/jquery.slim.js
    - Linea: 3265
    - Acciones: Remove this assignment of "firingIndex".

33. Componente: vendor/jquery/jquery.slim.js
    - Linea: 3272
    - Acciones: Remove this assignment of "firingIndex".

34. Componente: vendor/magnific-popup/jquery.magnific-popup.js
    - Linea: 47
    - Acciones: Unexpected empty function.

35. Componente: vendor/magnific-popup/jquery.magnific-popup.js
    - Linea: 156
    - Acciones: Refactor this function to reduce its Cognitive Complexity from 61 to the 15 allowed.

36. Componente: vendor/magnific-popup/jquery.magnific-popup.js
    - Linea: 633
    - Acciones: Refactor this function to reduce its Cognitive Complexity from 19 to the 15 allowed.

37. Componente: vendor/magnific-popup/jquery.magnific-popup.js
    - Linea: 713
    - Acciones: Refactor this function to reduce its Cognitive Complexity from 19 to the 15 allowed.

38. Componente: vendor/magnific-popup/jquery.magnific-popup.js
    - Linea: 766
    - Acciones: Refactor this function to reduce its Cognitive Complexity from 27 to the 15 allowed.

39. Componente: vendor/magnific-popup/jquery.magnific-popup.js
    - Linea: 909
    - Acciones: Refactor this function to reduce its Cognitive Complexity from 23 to the 15 allowed.

40. Componente: vendor/magnific-popup/jquery.magnific-popup.js
    - Linea: 1248
    - Acciones: Refactor this function to reduce its Cognitive Complexity from 36 to the 15 allowed.

41. Componente: vendor/magnific-popup/jquery.magnific-popup.js
    - Linea: 1381
    - Acciones: Refactor this function to reduce its Cognitive Complexity from 21 to the 15 allowed.

42. Componente: vendor/magnific-popup/jquery.magnific-popup.js
    - Linea: 1686
    - Acciones: Refactor this function to reduce its Cognitive Complexity from 21 to the 15

allowed.

Detalle de vulnerabilidades de tipo: Importantes

1. Componente: JavaScript/dic_cursos.js
   - Linea: 18
   - Acciones: Remove this useless assignment to variable "red".

2. Componente: JavaScript/dic_cursos.js
   - Linea: 20
   - Acciones: Remove this useless assignment to variable "yellow".

3. Componente: JavaScript/fb_sdk.js
   - Linea: 22
   - Acciones: This statement will not be executed conditionally; only the first statement will be. The rest will execute unconditionally.

4. Componente: JavaScript/fb_sdk.js
   - Linea: 22
   - Acciones: This statement will not be executed conditionally; only the first statement will be. The rest will execute unconditionally.

5. Componente: JavaScript/fb_sdk.js
   - Linea: 22
   - Acciones: 'a' is already declared in the upper scope.

6. Componente: JavaScript/fb_sdk.js
   - Linea: 22
   - Acciones: 'b' is already declared in the upper scope.

7. Componente: JavaScript/fb_sdk.js
   - Linea: 22
   - Acciones: 'd' is already declared in the upper scope.

8. Componente: JavaScript/fb_sdk.js
   - Linea: 22
   - Acciones: 'b' is already declared in the upper scope.

9. Componente: JavaScript/fb_sdk.js
   - Linea: 22
   - Acciones: 'a' is already declared in the upper scope.

10. Componente: JavaScript/fb_sdk.js
   - Linea: 22
   - Acciones: 'd' is already declared in the upper scope.

11. Componente: JavaScript/fb_sdk.js
   - Linea: 22
   - Acciones: This statement will not be executed in a loop; only the first statement will be. The rest will execute only once.

12. Componente: JavaScript/fb_sdk.js
   - Linea: 22
   - Acciones: 'a' is already declared in the upper scope.

13. Componente: JavaScript/fb_sdk.js
   - Linea: 22
   - Acciones: 'b' is already defined.

14. Componente: JavaScript/fb_sdk.js
   - Linea: 22
   - Acciones: This statement will not be executed conditionally; only the first statement will be. The rest will execute unconditionally.

15. Componente: JavaScript/fb_sdk.js
   - Linea: 22
   - Acciones: This statement will not be executed in a loop; only the first statement will be. The rest will execute only once.

16. Componente: JavaScript/fb_sdk.js
   - Linea: 22
   - Acciones: 'a' is already declared in the upper scope.

17. Componente: JavaScript/fb_sdk.js
   - Linea: 22
   - Acciones: Remove this "===" check; it will always be false. Did you mean to use "=="?

18. Componente: JavaScript/fb_sdk.js
    - Linea: 22
    - Acciones: This statement will not be executed conditionally; only the first statement will be. The rest will execute unconditionally.

19. Componente: JavaScript/fb_sdk.js
    - Linea: 22
    - Acciones: Use "indexOf" or "includes" (available from ES2016) instead.

20. Componente: JavaScript/jqBootstrapValidation.js
    - Linea: 27
    - Acciones: Remove this commented out code.

21. Componente: JavaScript/jqBootstrapValidation.js
    - Linea: 266
    - Acciones: 'i' is already declared in the upper scope.

22. Componente: JavaScript/jqBootstrapValidation.js
    - Linea: 266
    - Acciones: 'el' is already declared in the upper scope.

23. Componente: JavaScript/jqBootstrapValidation.js
    - Linea: 287
    - Acciones: 'message' is already declared in the upper scope.

24. Componente: JavaScript/jqBootstrapValidation.js
    - Linea: 300
    - Acciones: 'validatorType' is already declared in the upper scope.

25. Componente: JavaScript/jqBootstrapValidation.js
    - Linea: 458
    - Acciones: 'message' is already declared in the upper scope.

26. Componente: JavaScript/jqBootstrapValidation.js
    - Linea: 471
    - Acciones: Move this array "sort" operation to a separate statement.

27. Componente: css/freelancer.css
    - Linea: 2
    - Acciones: Unexpected missing generic font family

28. Componente: css/freelancer.css
    - Linea: 12
    - Acciones: Unexpected missing generic font family

29. Componente: css/freelancer.css
    - Linea: 35
    - Acciones: Unexpected missing generic font family

30. Componente: css/freelancer.css
    - Linea: 102
    - Acciones: Unexpected missing generic font family

31. Componente: css/freelancer.css
    - Linea: 181
    - Acciones: Unexpected missing generic font family

32. Componente: gym/crud.php
    - Linea: 18
    - Acciones: Delete this unreachable code or refactor the code to make it reachable.

33. Componente: gym/crud.php
    - Linea: 31
    - Acciones: Delete this unreachable code or refactor the code to make it reachable.

34. Componente: gym/crud.php
    - Linea: 41
    - Acciones: Delete this unreachable code or refactor the code to make it reachable.

35. Componente: gym/crud.php
    - Linea: 50
    - Acciones: Delete this unreachable code or refactor the code to make it reachable.

36. Componente: gym/crud.php
    - Linea: 58

- Acciones: Delete this unreachable code or refactor the code to make it reachable.

37. Componente: gym/crud.php
    - Linea: 67
    - Acciones: Delete this unreachable code or refactor the code to make it reachable.

38. Componente: gym/evaluacion.php
    - Linea: 3
    - Acciones: Remove this commented out code.

39. Componente: gym/evaluacion.php
    - Linea: 10
    - Acciones: Insert a <!DOCTYPE> declaration to before this <html> tag.

40. Componente: gym/evaluacion.php
    - Linea: 10
    - Acciones: Add "lang" and/or "xml:lang" attributes to this "<html>" element

41. Componente: gym/evaluacion.php
    - Linea: 11
    - Acciones: Add a <title> tag to this page.

42. Componente: gym/logout.php
    - Linea: 25
    - Acciones: This branch's code block is the same as the block for the branch on line 4.

43. Componente: gym/registro.php
    - Linea: 7
    - Acciones: Add "lang" and/or "xml:lang" attributes to this "<html>" element

44. Componente: gym/rutinas.php
    - Linea: 9
    - Acciones: Remove this commented out code.

45. Componente: gym/rutinas.php
    - Linea: 18
    - Acciones: Add "lang" and/or "xml:lang" attributes to this "<html>" element

46. Componente: gym/visualizador.php
    - Linea: 9
    - Acciones: Remove this commented out code.

47. Componente: gym/visualizador.php
    - Linea: 17
    - Acciones: Add "lang" and/or "xml:lang" attributes to this "<html>" element

48. Componente: index.html
    - Linea: 169
    - Acciones: Remove this commented out code.

49. Componente: scss/_global.scss
    - Linea: 36
    - Acciones: Unexpected missing generic font family

50. Componente: scss/_mixins.scss
    - Linea: 2
    - Acciones: Unexpected missing generic font family

51. Componente: scss/_mixins.scss
    - Linea: 7
    - Acciones: Unexpected missing generic font family

52. Componente: vendor/bootstrap/css/bootstrap-reboot.css
    - Linea: 66
    - Acciones: Unexpected duplicate "text-decoration"

53. Componente: vendor/bootstrap/css/bootstrap-reboot.css
    - Linea: 163
    - Acciones: Unexpected duplicate name monospace

54. Componente: vendor/bootstrap/css/bootstrap.css
    - Linea: 96
    - Acciones: Unexpected duplicate "text-decoration"

55. Componente: vendor/bootstrap/css/bootstrap.css
    - Linea: 423

- Acciones: Unexpected duplicate selector "hr", first used at line 76

56. Componente: vendor/bootstrap/css/bootstrap.css
    - Linea: 532
    - Acciones: Unexpected duplicate selector "pre", first used at line 197

57. Componente: vendor/bootstrap/css/bootstrap.css
    - Linea: 3090
    - Acciones: Unexpected duplicate selector ".dropright .dropdown-toggle::after", first used at line 3073

58. Componente: vendor/bootstrap/css/bootstrap.css
    - Linea: 3111
    - Acciones: Unexpected duplicate selector ".dropleft .dropdown-toggle::after", first used at line 3102

59. Componente: vendor/bootstrap/css/bootstrap.css
    - Linea: 3131
    - Acciones: Unexpected duplicate selector ".dropleft .dropdown-toggle::before", first used at line 3115

60. Componente: vendor/bootstrap/css/bootstrap.css
    - Linea: 4220
    - Acciones: Unexpected duplicate selector ".navbar-expand > .container, .navbar-expand > .container-fluid", first used at line 4200 (no-duplicate-selectors)

61. Componente: vendor/bootstrap/css/bootstrap.css
    - Linea: 4624
    - Acciones: Unexpected duplicate selector ".breadcrumb-item + .breadcrumb-item:hover::before", first used at line 4620

62. Componente: vendor/bootstrap/css/bootstrap.css
    - Linea: 8888
    - Acciones: Unexpected missing generic font family

63. Componente: vendor/bootstrap/js/bootstrap.bundle.js
    - Linea: 8
    - Acciones: Extract this nested ternary operation into an independent statement.

64. Componente: vendor/bootstrap/js/bootstrap.bundle.js
    - Linea: 15
    - Acciones: 'i' is already declared in the upper scope.

65. Componente: vendor/bootstrap/js/bootstrap.bundle.js
    - Linea: 46
    - Acciones: 'i' is already declared in the upper scope.

66. Componente: vendor/bootstrap/js/bootstrap.bundle.js
    - Linea: 131
    - Acciones: 'Util' is already declared in the upper scope.

67. Componente: vendor/bootstrap/js/bootstrap.bundle.js
    - Linea: 242
    - Acciones: 'Alert' is already declared in the upper scope.

68. Componente: vendor/bootstrap/js/bootstrap.bundle.js
    - Linea: 245
    - Acciones: 'Alert' is already declared in the upper scope.

69. Componente: vendor/bootstrap/js/bootstrap.bundle.js
    - Linea: 420
    - Acciones: 'Button' is already declared in the upper scope.

70. Componente: vendor/bootstrap/js/bootstrap.bundle.js
    - Linea: 423
    - Acciones: 'Button' is already declared in the upper scope.

71. Componente: vendor/bootstrap/js/bootstrap.bundle.js
    - Linea: 623
    - Acciones: 'Carousel' is already declared in the upper scope.

72. Componente: vendor/bootstrap/js/bootstrap.bundle.js
    - Linea: 626
    - Acciones: 'Carousel' is already declared in the upper scope.

73. Componente: vendor/bootstrap/js/bootstrap.bundle.js

- Linea: 1098
- Acciones: 'Collapse' is already declared in the upper scope.

74. Componente: vendor/bootstrap/js/bootstrap.bundle.js
    - Linea: 1101
    - Acciones: 'Collapse' is already declared in the upper scope.

75. Componente: vendor/bootstrap/js/bootstrap.bundle.js
    - Linea: 1108
    - Acciones: 'i' is already declared in the upper scope.

76. Componente: vendor/bootstrap/js/bootstrap.bundle.js
    - Linea: 1210
    - Acciones: 'hide' is already declared in the upper scope.

77. Componente: vendor/bootstrap/js/bootstrap.bundle.js
    - Linea: 1231
    - Acciones: 'i' is already declared in the upper scope.

78. Componente: vendor/bootstrap/js/bootstrap.bundle.js
    - Linea: 1301
    - Acciones: 'i' is already declared in the upper scope.

79. Componente: vendor/bootstrap/js/bootstrap.bundle.js
    - Linea: 1742
    - Acciones: Extract this nested ternary operation into an independent statement.

80. Componente: vendor/bootstrap/js/bootstrap.bundle.js
    - Linea: 1742
    - Acciones: Extract this nested ternary operation into an independent statement.

81. Componente: vendor/bootstrap/js/bootstrap.bundle.js
    - Linea: 1763
    - Acciones: Update this function so that its implementation is not identical to the one on line 14.

82. Componente: vendor/bootstrap/js/bootstrap.bundle.js
    - Linea: 1764

- Acciones: 'i' is already declared in the upper scope.

83. Componente: vendor/bootstrap/js/bootstrap.bundle.js
    - Linea: 1784
    - Acciones: Update this function so that its implementation is not identical to the one on line 30.

84. Componente: vendor/bootstrap/js/bootstrap.bundle.js
    - Linea: 1800
    - Acciones: 'i' is already declared in the upper scope.

85. Componente: vendor/bootstrap/js/bootstrap.bundle.js
    - Linea: 1886
    - Acciones: 'isIE10' is already declared in the upper scope.

86. Componente: vendor/bootstrap/js/bootstrap.bundle.js
    - Linea: 1946
    - Acciones: 'offset' is already declared in the upper scope.

87. Componente: vendor/bootstrap/js/bootstrap.bundle.js
    - Linea: 2015
    - Acciones: Remove this "===" check; it will always be false. Did you mean to use "=="?

88. Componente: vendor/bootstrap/js/bootstrap.bundle.js
    - Linea: 2020
    - Acciones: Remove this "===" check; it will always be false. Did you mean to use "=="?

89. Componente: vendor/bootstrap/js/bootstrap.bundle.js
    - Linea: 2025
    - Acciones: Remove this "===" check; it will always be false. Did you mean to use "=="?

90. Componente: vendor/bootstrap/js/bootstrap.bundle.js
    - Linea: 2266
    - Acciones: 'modifiers' is already declared in the upper scope.

91. Componente: vendor/bootstrap/js/bootstrap.bundle.js
    - Linea: 2348
    - Acciones: 'modifiers' is already declared in the upper scope.

92. Componente: vendor/bootstrap/js/bootstrap.bundle.js
    - Linea: 2367
    - Acciones: 'i' is already declared in the upper scope.

93. Componente: vendor/bootstrap/js/bootstrap.bundle.js
    - Linea: 2708
    - Acciones: 'modifiers' is already declared in the upper scope.

94. Componente: vendor/bootstrap/js/bootstrap.bundle.js
    - Linea: 3067
    - Acciones: 'offset' is already declared in the upper scope.

95. Componente: vendor/bootstrap/js/bootstrap.bundle.js
    - Linea: 3099
    - Acciones: Extract this nested ternary operation into an independent statement.

96. Componente: vendor/bootstrap/js/bootstrap.bundle.js
    - Linea: 3144
    - Acciones: 'offset' is already declared in the upper scope.

97. Componente: vendor/bootstrap/js/bootstrap.bundle.js
    - Linea: 3337
    - Acciones: Extract this nested ternary operation into an independent statement.

98. Componente: vendor/bootstrap/js/bootstrap.bundle.js
    - Linea: 3766
    - Acciones: Remove this commented out code.

99. Componente: vendor/bootstrap/js/bootstrap.bundle.js
    - Linea: 3777
    - Acciones: 'Popper' is already declared in the upper scope.

100. Componente: vendor/bootstrap/js/bootstrap.bundle.js
    - Linea: 4011
    - Acciones: 'Dropdown' is already declared in the upper scope.

Detalle de vulnerabilidades de tipo: Menores

1. Componente: JavaScript/dic_cursos.js
   - Linea: 18
   - Acciones: Remove the declaration of the unused 'red' variable.

2. Componente: JavaScript/dic_cursos.js
   - Linea: 20
   - Acciones: Remove the declaration of the unused 'yellow' variable.

3. Componente: JavaScript/fb_sdk.js
   - Linea: 22
   - Acciones: Expected a `for-of` loop instead of a `for` loop with this simple iteration.

4. Componente: JavaScript/fb_sdk.js
   - Linea: 22
   - Acciones: Expected a `for-of` loop instead of a `for` loop with this simple iteration.

5. Componente: JavaScript/jqBootstrapValidation.js
   - Linea: 889
   - Acciones: Expected a `for-of` loop instead of a `for` loop with this simple iteration.

6. Componente: gym/conexion.php
   - Linea: 13
   - Acciones: Immediately return this expression instead of assigning it to the temporary variable "$conexion".

7. Componente: gym/crud.php
   - Linea: 16
   - Acciones: Immediately return this expression instead of assigning it to the temporary variable "$nfilas".

8. Componente: gym/crud.php
   - Linea: 26
   - Acciones: Replace this "if-then-else" statement by a single "return" statement.

9. Componente: gym/crud.php
   - Linea: 39
   - Acciones: Immediately return this expression instead of assigning it to the temporary

variable "$mediciones".

10. Componente: gym/crud.php
    - Linea: 48
    - Acciones: Immediately return this expression instead of assigning it to the temporary variable "$rutinas".

11. Componente: gym/crud.php
    - Linea: 56
    - Acciones: Immediately return this expression instead of assigning it to the temporary variable "$mediciones".

12. Componente: gym/crud.php
    - Linea: 65
    - Acciones: Immediately return this expression instead of assigning it to the temporary variable "$nfilas".

13. Componente: gym/rutinas.php
    - Linea: 43
    - Acciones: Add a description to this table.

14. Componente: gym/visualizador.php
    - Linea: 148
    - Acciones: Add a description to this table.

15. Componente: index.html
    - Linea: 64
    - Acciones: Replace this <i> tag by .

16. Componente: index.html
    - Linea: 94
    - Acciones: Replace this <i> tag by .

17. Componente: index.html
    - Linea: 99
    - Acciones: Replace this <i> tag by .

18. Componente: index.html

- Linea: 104
- Acciones: Replace this <i> tag by .

19. Componente: index.html
    - Linea: 271
    - Acciones: Replace this <i> tag by .

20. Componente: index.html
    - Linea: 272
    - Acciones: Replace this <i> tag by .

21. Componente: index.html
    - Linea: 283
    - Acciones: Replace this <i> tag by .

22. Componente: index.html
    - Linea: 284
    - Acciones: Replace this <i> tag by .

23. Componente: index.html
    - Linea: 296
    - Acciones: Replace this <i> tag by .

24. Componente: index.html
    - Linea: 297
    - Acciones: Replace this <i> tag by .

25. Componente: index.html
    - Linea: 308
    - Acciones: Replace this <i> tag by .

26. Componente: index.html
    - Linea: 309
    - Acciones: Replace this <i> tag by .

27. Componente: index.html
    - Linea: 358
    - Acciones: Replace this <i> tag by .

28. Componente: index.html
    - Linea: 366
    - Acciones: Replace this <i> tag by .

29. Componente: index.html
    - Linea: 378
    - Acciones: Replace this <i> tag by .

30. Componente: index.html
    - Linea: 392
    - Acciones: Replace this <i> tag by .

31. Componente: index.html
    - Linea: 469
    - Acciones: Replace this <i> tag by .

32. Componente: index.html
    - Linea: 474
    - Acciones: Replace this <i> tag by .

33. Componente: index.html
    - Linea: 479
    - Acciones: Replace this <i> tag by .

34. Componente: index.html
    - Linea: 483
    - Acciones: Replace this <i> tag by .

35. Componente: index.html
    - Linea: 490
    - Acciones: Replace this <i> tag by .

36. Componente: index.html
    - Linea: 490
    - Acciones: Replace this <i> tag by .

37. Componente: index.html

- Linea: 491
- Acciones: Replace this <i> tag by .

38. Componente: index.html
    - Linea: 491
    - Acciones: Replace this <i> tag by .

39. Componente: index.html
    - Linea: 507
    - Acciones: Replace this <i> tag by .

40. Componente: index.html
    - Linea: 517
    - Acciones: Replace this <i> tag by .

41. Componente: index.html
    - Linea: 546
    - Acciones: Replace this <i> tag by .

42. Componente: index.html
    - Linea: 558
    - Acciones: Replace this <i> tag by .

43. Componente: index.html
    - Linea: 587
    - Acciones: Replace this <i> tag by .

44. Componente: index.html
    - Linea: 599
    - Acciones: Replace this <i> tag by .

45. Componente: index.html
    - Linea: 628
    - Acciones: Replace this <i> tag by .

46. Componente: index.html
    - Linea: 642
    - Acciones: Replace this <i> tag by .

47. Componente: index.html
    - Linea: 688
    - Acciones: Replace this <i> tag by .

48. Componente: index.html
    - Linea: 702
    - Acciones: Replace this <i> tag by .

49. Componente: index.html
    - Linea: 753
    - Acciones: Replace this <i> tag by .

50. Componente: vendor/bootstrap/js/bootstrap.bundle.js
    - Linea: 15
    - Acciones: Expected a `for-of` loop instead of a `for` loop with this simple iteration.

51. Componente: vendor/bootstrap/js/bootstrap.bundle.js
    - Linea: 1108
    - Acciones: Expected a `for-of` loop instead of a `for` loop with this simple iteration.

52. Componente: vendor/bootstrap/js/bootstrap.bundle.js
    - Linea: 1231
    - Acciones: Expected a `for-of` loop instead of a `for` loop with this simple iteration.

53. Componente: vendor/bootstrap/js/bootstrap.bundle.js
    - Linea: 1431
    - Acciones: Expected a `for-of` loop instead of a `for` loop with this simple iteration.

54. Componente: vendor/bootstrap/js/bootstrap.bundle.js
    - Linea: 1764
    - Acciones: Expected a `for-of` loop instead of a `for` loop with this simple iteration.

55. Componente: vendor/bootstrap/js/bootstrap.bundle.js
    - Linea: 2153
    - Acciones: Immediately return this expression instead of assigning it to the temporary variable "result".

56. Componente: vendor/bootstrap/js/bootstrap.bundle.js
    - Linea: 2367
    - Acciones: Expected a `for-of` loop instead of a `for` loop with this simple iteration.

57. Componente: vendor/bootstrap/js/bootstrap.bundle.js
    - Linea: 4241
    - Acciones: Expected a `for-of` loop instead of a `for` loop with this simple iteration.

58. Componente: vendor/bootstrap/js/bootstrap.js
    - Linea: 16
    - Acciones: Expected a `for-of` loop instead of a `for` loop with this simple iteration.

59. Componente: vendor/bootstrap/js/bootstrap.js
    - Linea: 1109
    - Acciones: Expected a `for-of` loop instead of a `for` loop with this simple iteration.

60. Componente: vendor/bootstrap/js/bootstrap.js
    - Linea: 1232
    - Acciones: Expected a `for-of` loop instead of a `for` loop with this simple iteration.

61. Componente: vendor/bootstrap/js/bootstrap.js
    - Linea: 1724
    - Acciones: Expected a `for-of` loop instead of a `for` loop with this simple iteration.

62. Componente: vendor/jquery/jquery.js
    - Linea: 2100
    - Acciones: Replace this "for" loop with a "while" loop.

63. Componente: vendor/jquery/jquery.js
    - Linea: 2108
    - Acciones: Replace this "for" loop with a "while" loop.

64. Componente: vendor/jquery/jquery.js
    - Linea: 2807
    - Acciones: Unnecessary semicolon.

65. Componente: vendor/jquery/jquery.slim.js
    - Linea: 2100

- Acciones: Replace this "for" loop with a "while" loop.

66. Componente: vendor/jquery/jquery.slim.js
    - Linea: 2108
    - Acciones: Replace this "for" loop with a "while" loop.

67. Componente: vendor/jquery/jquery.slim.js
    - Linea: 2807
    - Acciones: Unnecessary semicolon.

68. Componente: vendor/magnific-popup/jquery.magnific-popup.js
    - Linea: 4
    - Acciones: Unnecessary semicolon.

69. Componente: vendor/magnific-popup/jquery.magnific-popup.js
    - Linea: 581
    - Acciones: Expected a `for-of` loop instead of a `for` loop with this simple iteration.

Detalle de vulnerabilidades de tipo: Información

1. Componente: vendor/bootstrap/js/bootstrap.bundle.js
    - Linea: 178
    - Acciones: Complete the task associated to this "TODO" comment.

2. Componente: vendor/bootstrap/js/bootstrap.bundle.js
    - Linea: 4795
    - Acciones: Complete the task associated to this "TODO" comment.

3. Componente: vendor/bootstrap/js/bootstrap.bundle.js
    - Linea: 5954
    - Acciones: Complete the task associated to this "TODO" comment.

4. Componente: vendor/bootstrap/js/bootstrap.js
    - Linea: 179
    - Acciones: Complete the task associated to this "TODO" comment.

5. Componente: vendor/bootstrap/js/bootstrap.js
    - Linea: 2278

- Acciones: Complete the task associated to this "TODO" comment.

6. Componente: vendor/bootstrap/js/bootstrap.js
   - Linea: 3437
   - Acciones: Complete the task associated to this "TODO" comment.

7. Componente: vendor/jquery/jquery.js
   - Linea: 753
   - Acciones: Complete the task associated to this "TODO" comment.

8. Componente: vendor/jquery/jquery.js
   - Linea: 767
   - Acciones: Complete the task associated to this "TODO" comment.

9. Componente: vendor/jquery/jquery.js
   - Linea: 4166
   - Acciones: Complete the task associated to this "TODO" comment.

10. Componente: vendor/jquery/jquery.js
    - Linea: 4234
    - Acciones: Complete the task associated to this "TODO" comment.

11. Componente: vendor/jquery/jquery.slim.js
    - Linea: 753
    - Acciones: Complete the task associated to this "TODO" comment.

12. Componente: vendor/jquery/jquery.slim.js
    - Linea: 767
    - Acciones: Complete the task associated to this "TODO" comment.

13. Componente: vendor/jquery/jquery.slim.js
    - Linea: 4166
    - Acciones: Complete the task associated to this "TODO" comment.

14. Componente: vendor/jquery/jquery.slim.js
    - Linea: 4234
    - Acciones: Complete the task associated to this "TODO" comment.

15. Componente: vendor/magnific-popup/jquery.magnific-popup.js
    - Linea: 1310
    - Acciones: Complete the task associated to this "TODO" comment.

5.1.2 Trivy.

Trivy	
Severidad	**Cantidad**
Críticas	2
Altas	24
Medias	12
Bajas	90
Desconocidas	0

Detalle de vulnerabilidades de tipo: Críticas

1. Librería: libgnutls30
   - Versión: 3.6.7-4+deb10u6
   - Id de vulnerabilidad: CVE-2021-20231
   - Mensaje: A flaw was found in gnutls. A use after free issue in client sending key_share extension may lead to memory corruption and other consequences.
   - Fuente: https://avd.aquasec.com/nvd/cve-2021-20231

2. Librería: libgnutls30
   - Versión: 3.6.7-4+deb10u6
   - Id de vulnerabilidad: CVE-2021-20232
   - Mensaje: A flaw was found in gnutls. A use after free issue in client_send_params in lib/ext/pre_shared_key.c may lead to memory corruption and other potential consequences.
   - Fuente: https://avd.aquasec.com/nvd/cve-2021-20232

Detalle de vulnerabilidades de tipo: Altas

1. Librería: gcc-8-base
   - Versión: 8.3.0-6
   - Id de vulnerabilidad: CVE-2018-12886
   - Mensaje: stack_protect_prologue in cfgexpand.c and stack_protect_epilogue in function.c in GNU Compiler Collection (GCC) 4.1 through 8 (under certain circumstances) generate instruction sequences when targeting ARM targets that spill the address of the stack protector guard, which allows an attacker to bypass the protection of -fstack-protector, -fstack-protector-all, -fstack-protector-strong, and -fstack-protector-explicit against stack overflow by controlling what the stack

canary is compared against.

- Fuente: https://avd.aquasec.com/nvd/cve-2018-12886

2. Librería: gcc-8-base
   - Versión: 8.3.0-6
   - Id de vulnerabilidad: CVE-2019-15847
   - Mensaje: The POWER9 backend in GNU Compiler Collection (GCC) before version 10 could optimize multiple calls of the __builtin_darn intrinsic into a single call, thus reducing the entropy of the random number generator. This occurred because a volatile operation was not specified. For example, within a single execution of a program, the output of every __builtin_darn() call may be the same.
   - Fuente: https://avd.aquasec.com/nvd/cve-2019-15847

3. Librería: libc-bin
   - Versión: 2.28-10
   - Id de vulnerabilidad: CVE-2020-1751
   - Mensaje: An out-of-bounds write vulnerability was found in glibc before 2.31 when handling signal trampolines on PowerPC. Specifically, the backtrace function did not properly check the array bounds when storing the frame address, resulting in a denial of service or potential code execution. The highest threat from this vulnerability is to system availability.
   - Fuente: https://avd.aquasec.com/nvd/cve-2020-1751

4. Librería: libc-bin
   - Versión: 2.28-10
   - Id de vulnerabilidad: CVE-2020-1752
   - Mensaje: A use-after-free vulnerability introduced in glibc upstream version 2.14 was found in the way the tilde expansion was carried out. Directory paths containing an initial tilde followed by a valid username were affected by this issue. A local attacker could exploit this flaw by creating a specially crafted path that, when processed by the glob function, would potentially lead to arbitrary code execution. This was fixed in version 2.32.
   - Fuente: https://avd.aquasec.com/nvd/cve-2020-1752

5. Librería: libc-bin
   - Versión: 2.28-10
   - Id de vulnerabilidad: CVE-2021-3326
   - Mensaje: The iconv function in the GNU C Library (aka glibc or libc6) 2.32 and earlier, when processing invalid input sequences in the ISO-2022-JP-3 encoding, fails an assertion in the code path and aborts the program, potentially resulting in a denial of service.

- Fuente: https://avd.aquasec.com/nvd/cve-2021-3326

6. Librería: libc6
   - Versión: 2.28-10
   - Id de vulnerabilidad: CVE-2020-1751
   - Mensaje: An out-of-bounds write vulnerability was found in glibc before 2.31 when handling signal trampolines on PowerPC. Specifically, the backtrace function did not properly check the array bounds when storing the frame address, resulting in a denial of service or potential code execution. The highest threat from this vulnerability is to system availability.
   - Fuente: https://avd.aquasec.com/nvd/cve-2020-1751

7. Librería: libc6
   - Versión: 2.28-10
   - Id de vulnerabilidad: CVE-2020-1752
   - Mensaje: A use-after-free vulnerability introduced in glibc upstream version 2.14 was found in the way the tilde expansion was carried out. Directory paths containing an initial tilde followed by a valid username were affected by this issue. A local attacker could exploit this flaw by creating a specially crafted path that, when processed by the glob function, would potentially lead to arbitrary code execution. This was fixed in version 2.32.
   - Fuente: https://avd.aquasec.com/nvd/cve-2020-1752

8. Librería: libc6
   - Versión: 2.28-10
   - Id de vulnerabilidad: CVE-2021-3326
   - Mensaje: The iconv function in the GNU C Library (aka glibc or libc6) 2.32 and earlier, when processing invalid input sequences in the ISO-2022-JP-3 encoding, fails an assertion in the code path and aborts the program, potentially resulting in a denial of service.
   - Fuente: https://avd.aquasec.com/nvd/cve-2021-3326

9. Librería: libgcc1
   - Versión: 8.3.0-6
   - Id de vulnerabilidad: CVE-2018-12886
   - Mensaje: stack_protect_prologue in cfgexpand.c and stack_protect_epilogue in function.c in GNU Compiler Collection (GCC) 4.1 through 8 (under certain circumstances) generate instruction sequences when targeting ARM targets that spill the address of the stack protector guard, which allows an attacker to bypass the protection of -fstack-protector, -fstack-protector-all, -fstack-protector-strong, and -fstack-protector-explicit against stack overflow by controlling what the stack canary is compared against.

- Fuente: https://avd.aquasec.com/nvd/cve-2018-12886

10. Librería: libgcc1
    - Versión: 8.3.0-6
    - Id de vulnerabilidad: CVE-2019-15847
    - Mensaje: The POWER9 backend in GNU Compiler Collection (GCC) before version 10 could optimize multiple calls of the __builtin_darn intrinsic into a single call, thus reducing the entropy of the random number generator. This occurred because a volatile operation was not specified. For example, within a single execution of a program, the output of every __builtin_darn() call may be the same.
    - Fuente: https://avd.aquasec.com/nvd/cve-2019-15847

11. Librería: libgnutls30
    - Versión: 3.6.7-4+deb10u6
    - Id de vulnerabilidad: CVE-2020-24659
    - Mensaje: An issue was discovered in GnuTLS before 3.6.15. A server can trigger a NULL pointer dereference in a TLS 1.3 client if a no_renegotiation alert is sent with unexpected timing, and then an invalid second handshake occurs. The crash happens in the application's error handling path, where the gnutls_deinit function is called after detecting a handshake failure.
    - Fuente: https://avd.aquasec.com/nvd/cve-2020-24659

12. Librería: libhogweed4
    - Versión: 3.4.1-1
    - Id de vulnerabilidad: CVE-2021-20305
    - Mensaje: A flaw was found in Nettle in versions before 3.7.2, where several Nettle signature verification functions (GOST DSA, EDDSA & ECDSA) result in the Elliptic Curve Cryptography point (ECC) multiply function being called with out-of-range scalers, possibly resulting in incorrect results. This flaw allows an attacker to force an invalid signature, causing an assertion failure or possible validation. The highest threat to this vulnerability is to confidentiality, integrity, as well as system availability.
    - Fuente: https://avd.aquasec.com/nvd/cve-2021-20305

13. Librería: libidn2-0
    - Versión: 2.0.5-1+deb10u1
    - Id de vulnerabilidad: CVE-2019-12290
    - Mensaje: GNU libidn2 before 2.2.0 fails to perform the roundtrip checks specified in RFC3490 Section 4.2 when converting A-labels to U-labels. This makes it possible in some circumstances for one domain to impersonate another. By creating a malicious domain that

matches a target domain except for the inclusion of certain punycoded Unicode characters (that would be discarded when converted first to a Unicode label and then back to an ASCII label), arbitrary domains can be impersonated.

- Fuente: https://avd.aquasec.com/nvd/cve-2019-12290

14. Librería: libnettle6
    - Versión: 3.4.1-1
    - Id de vulnerabilidad: CVE-2021-20305
    - Mensaje: A flaw was found in Nettle in versions before 3.7.2, where several Nettle signature verification functions (GOST DSA, EDDSA & ECDSA) result in the Elliptic Curve Cryptography point (ECC) multiply function being called with out-of-range scalers, possibly resulting in incorrect results. This flaw allows an attacker to force an invalid signature, causing an assertion failure or possible validation. The highest threat to this vulnerability is to confidentiality, integrity, as well as system availability.
    - Fuente: https://avd.aquasec.com/nvd/cve-2021-20305

15. Librería: libssh2-1
    - Versión: 1.8.0-2.1
    - Id de vulnerabilidad: CVE-2019-13115
    - Mensaje: In libssh2 before 1.9.0, kex_method_diffie_hellman_group_exchange_sha256_key_exchange in kex.c has an integer overflow that could lead to an out-of-bounds read in the way packets are read from the server. A remote attacker who compromises a SSH server may be able to disclose sensitive information or cause a denial of service condition on the client system when a user connects to the server. This is related to an _libssh2_check_length mistake, and is different from the various issues fixed in 1.8.1, such as CVE-2019-3855.
    - Fuente: https://avd.aquasec.com/nvd/cve-2019-13115

16. Librería: libstdc++6
    - Versión: 8.3.0-6
    - Id de vulnerabilidad: CVE-2018-12886
    - Mensaje: stack_protect_prologue in cfgexpand.c and stack_protect_epilogue in function.c in GNU Compiler Collection (GCC) 4.1 through 8 (under certain circumstances) generate instruction sequences when targeting ARM targets that spill the address of the stack protector guard, which allows an attacker to bypass the protection of -fstack-protector, -fstack-protector-all, -fstack-protector-strong, and -fstack-protector-explicit against stack overflow by controlling what the stack canary is compared against.
    - Fuente: https://avd.aquasec.com/nvd/cve-2018-12886

17. Librería: libstdc++6
    - Versión: 8.3.0-6
    - Id de vulnerabilidad: CVE-2019-15847
    - Mensaje: The POWER9 backend in GNU Compiler Collection (GCC) before version 10 could optimize multiple calls of the __builtin_darn intrinsic into a single call, thus reducing the entropy of the random number generator. This occurred because a volatile operation was not specified. For example, within a single execution of a program, the output of every __builtin_darn() call may be the same.
    - Fuente: https://avd.aquasec.com/nvd/cve-2019-15847

18. Librería: libsystemd0
    - Versión: 241-7~deb10u7
    - Id de vulnerabilidad: CVE-2019-3843
    - Mensaje: It was discovered that a systemd service that uses DynamicUser property can create a SUID/SGID binary that would be allowed to run as the transient service UID/GID even after the service is terminated. A local attacker may use this flaw to access resources that will be owned by a potentially different service in the future, when the UID/GID will be recycled.
    - Fuente: https://avd.aquasec.com/nvd/cve-2019-3843

19. Librería: libsystemd0
    - Versión: 241-7~deb10u7
    - Id de vulnerabilidad: CVE-2019-3844
    - Mensaje: It was discovered that a systemd service that uses DynamicUser property can get new privileges through the execution of SUID binaries, which would allow to create binaries owned by the service transient group with the setgid bit set. A local attacker may use this flaw to access resources that will be owned by a potentially different service in the future, when the GID will be recycled.
    - Fuente: https://avd.aquasec.com/nvd/cve-2019-3844

20. Librería: libudev1
    - Versión: 241-7~deb10u7
    - Id de vulnerabilidad: CVE-2019-3843
    - Mensaje: It was discovered that a systemd service that uses DynamicUser property can create a SUID/SGID binary that would be allowed to run as the transient service UID/GID even after the service is terminated. A local attacker may use this flaw to access resources that will be owned by a potentially different service in the future, when the UID/GID will be recycled.
    - Fuente: https://avd.aquasec.com/nvd/cve-2019-3843

21. Librería: libudev1
    - Versión: 241-7~deb10u7
    - Id de vulnerabilidad: CVE-2019-3844
    - Mensaje: It was discovered that a systemd service that uses DynamicUser property can get new privileges through the execution of SUID binaries, which would allow to create binaries owned by the service transient group with the setgid bit set. A local attacker may use this flaw to access resources that will be owned by a potentially different service in the future, when the GID will be recycled.
    - Fuente: https://avd.aquasec.com/nvd/cve-2019-3844

22. Librería: libxml2
    - Versión: 2.9.4+dfsg1-7+deb10u1
    - Id de vulnerabilidad: CVE-2017-16932
    - Mensaje: parser.c in libxml2 before 2.9.5 does not prevent infinite recursion in parameter entities.
    - Fuente: https://avd.aquasec.com/nvd/cve-2017-16932

23. Librería: libxml2
    - Versión: 2.9.4+dfsg1-7+deb10u1
    - Id de vulnerabilidad: CVE-2021-3517
    - Mensaje: There is a flaw in the xml entity encoding functionality of libxml2 in versions before 2.9.11. An attacker who is able to supply a crafted file to be processed by an application linked with the affected functionality of libxml2 could trigger an out-of-bounds read. The most likely impact of this flaw is to application availability, with some potential impact to confidentiality and integrity if an attacker is able to use memory information to further exploit the application.
    - Fuente: https://avd.aquasec.com/nvd/cve-2021-3517

24. Librería: libxml2
    - Versión: 2.9.4+dfsg1-7+deb10u1
    - Id de vulnerabilidad: CVE-2021-3518
    - Mensaje: There's a flaw in libxml2 in versions before 2.9.11. An attacker who is able to submit a crafted file to be processed by an application linked with libxml2 could trigger a use-after-free. The greatest impact from this flaw is to confidentiality, integrity, and availability.
    - Fuente: https://avd.aquasec.com/nvd/cve-2021-3518

Detalle de vulnerabilidades de tipo: Medias

1. Librería: libc-bin
   - Versión: 2.28-10
   - Id de vulnerabilidad: CVE-2019-25013
   - Mensaje: The iconv feature in the GNU C Library (aka glibc or libc6) through 2.32, when processing invalid multi-byte input sequences in the EUC-KR encoding, may have a buffer over-read.
   - Fuente: https://avd.aquasec.com/nvd/cve-2019-25013

2. Librería: libc-bin
   - Versión: 2.28-10
   - Id de vulnerabilidad: CVE-2020-10029
   - Mensaje: The GNU C Library (aka glibc or libc6) before 2.32 could overflow an on-stack buffer during range reduction if an input to an 80-bit long double function contains a non-canonical bit pattern, a seen when passing a 0x5d414141414141410000 value to sinl on x86 targets. This is related to sysdeps/ieee754/ldbl-96/e_rem_pio2l.c.
   - Fuente: https://avd.aquasec.com/nvd/cve-2020-10029

3. Librería: libc-bin
   - Versión: 2.28-10
   - Id de vulnerabilidad: CVE-2020-27618
   - Mensaje: The iconv function in the GNU C Library (aka glibc or libc6) 2.32 and earlier, when processing invalid multi-byte input sequences in IBM1364, IBM1371, IBM1388, IBM1390, and IBM1399 encodings, fails to advance the input state, which could lead to an infinite loop in applications, resulting in a denial of service, a different vulnerability from CVE-2016-10228.
   - Fuente: https://avd.aquasec.com/nvd/cve-2020-27618

4. Librería: libc6
   - Versión: 2.28-10
   - Id de vulnerabilidad: CVE-2019-25013
   - Mensaje: The iconv feature in the GNU C Library (aka glibc or libc6) through 2.32, when processing invalid multi-byte input sequences in the EUC-KR encoding, may have a buffer over-read.
   - Fuente: https://avd.aquasec.com/nvd/cve-2019-25013

5. Librería: libc6
   - Versión: 2.28-10
   - Id de vulnerabilidad: CVE-2020-10029
   - Mensaje: The GNU C Library (aka glibc or libc6) before 2.32 could overflow an on-stack

buffer during range reduction if an input to an 80-bit long double function contains a non-canonical bit pattern, a seen when passing a 0x5d414141414141410000 value to sinl on x86 targets. This is related to sysdeps/ieee754/ldbl-96/e_rem_pio2l.c.

- Fuente: https://avd.aquasec.com/nvd/cve-2020-10029

6. Librería: libc6
   - Versión: 2.28-10
   - Id de vulnerabilidad: CVE-2020-27618
   - Mensaje: The iconv function in the GNU C Library (aka glibc or libc6) 2.32 and earlier, when processing invalid multi-byte input sequences in IBM1364, IBM1371, IBM1388, IBM1390, and IBM1399 encodings, fails to advance the input state, which could lead to an infinite loop in applications, resulting in a denial of service, a different vulnerability from CVE-2016-10228.
   - Fuente: https://avd.aquasec.com/nvd/cve-2020-27618

7. Librería: libgcrypt20
   - Versión: 1.8.4-5
   - Id de vulnerabilidad: CVE-2019-13627
   - Mensaje: It was discovered that there was a ECDSA timing attack in the libgcrypt20 cryptographic library. Version affected: 1.8.4-5, 1.7.6-2+deb9u3, and 1.6.3-2+deb8u4. Versions fixed: 1.8.5-2 and 1.6.3-2+deb8u7.
   - Fuente: https://avd.aquasec.com/nvd/cve-2019-13627

8. Librería: libpcre3
   - Versión: 2:8.39-12
   - Id de vulnerabilidad: CVE-2020-14155
   - Mensaje: libpcre in PCRE before 8.44 allows an integer overflow via a large number after a (?C substring.
   - Fuente: https://avd.aquasec.com/nvd/cve-2020-14155

9. Librería: libxml2
   - Versión: 2.9.4+dfsg1-7+deb10u1
   - Id de vulnerabilidad: CVE-2016-9318
   - Mensaje: libxml2 2.9.4 and earlier, as used in XMLSec 1.2.23 and earlier and other products, does not offer a flag directly indicating that the current document may be read but other files may not be opened, which makes it easier for remote attackers to conduct XML External Entity (XXE) attacks via a crafted document.
   - Fuente: https://avd.aquasec.com/nvd/cve-2016-9318

10. Librería: libxml2
    - Versión: 2.9.4+dfsg1-7+deb10u1
    - Id de vulnerabilidad: CVE-2021-3516
    - Mensaje: There's a flaw in libxml2's xmllint. An attacker who is able to submit a crafted file to be processed by xmllint could trigger a use-after-free. The greatest impact of this flaw is to confidentiality, integrity, and availability.
    - Fuente: https://avd.aquasec.com/nvd/cve-2021-3516

11. Librería: libxml2
    - Versión: 2.9.4+dfsg1-7+deb10u1
    - Id de vulnerabilidad: CVE-2021-3537
    - Mensaje: A vulnerability found in libxml2 in versions before 2.9.11 shows that it did not propagate errors while parsing XML mixed content, causing a NULL dereference. If an untrusted XML document was parsed in recovery mode and post-validated, the flaw could be used to crash the application. The highest threat from this vulnerability is to system availability.
    - Fuente: https://avd.aquasec.com/nvd/cve-2021-3537

12. Librería: libxml2
    - Versión: 2.9.4+dfsg1-7+deb10u1
    - Id de vulnerabilidad: CVE-2021-3541
    - Mensaje: No description is available for this CVE.
    - Fuente: https://avd.aquasec.com/nvd/cve-2021-3541

Detalle de vulnerabilidades de tipo: Bajas

1. Librería: apt
    - Versión: 1.8.2.3
    - Id de vulnerabilidad: CVE-2011-3374
    - Mensaje: It was found that apt-key in apt, all versions, do not correctly validate gpg keys with the master keyring, leading to a potential man-in-the-middle attack.
    - Fuente: https://avd.aquasec.com/nvd/cve-2011-3374

2. Librería: bash
    - Versión: 5.0-4
    - Id de vulnerabilidad: CVE-2019-18276
    - Mensaje: An issue was discovered in disable_priv_mode in shell.c in GNU Bash through 5.0 patch 11. By default, if Bash is run with its effective UID not equal to its real UID, it will drop privileges by setting its effective UID to its real UID. However, it does so incorrectly. On Linux and

other systems that support "saved UID" functionality, the saved UID is not dropped. An attacker with command execution in the shell can use "enable -f" for runtime loading of a new builtin, which can be a shared object that calls setuid() and therefore regains privileges. However, binaries running with an effective UID of 0 are unaffected.

- Fuente: https://avd.aquasec.com/nvd/cve-2019-18276

3. Librería: bash
   - Versión: 5.0-4
   - Id de vulnerabilidad: TEMP-0841856-B18BAF
   - Mensaje: null
   - Fuente: https://security-tracker.debian.org/tracker/TEMP-0841856-B18BAF

4. Librería: coreutils
   - Versión: 8.30-3
   - Id de vulnerabilidad: CVE-2016-2781
   - Mensaje: chroot in GNU coreutils, when used with --userspec, allows local users to escape to the parent session via a crafted TIOCSTI ioctl call, which pushes characters to the terminal's input buffer.
   - Fuente: https://avd.aquasec.com/nvd/cve-2016-2781

5. Librería: coreutils
   - Versión: 8.30-3
   - Id de vulnerabilidad: CVE-2017-18018
   - Mensaje: In GNU Coreutils through 8.29, chown-core.c in chown and chgrp does not prevent replacement of a plain file with a symlink during use of the POSIX "-R -L" options, which allows local users to modify the ownership of arbitrary files by leveraging a race condition.
   - Fuente: https://avd.aquasec.com/nvd/cve-2017-18018

6. Librería: gpgv
   - Versión: 2.2.12-1+deb10u1
   - Id de vulnerabilidad: CVE-2019-14855
   - Mensaje: A flaw was found in the way certificate signatures could be forged using collisions found in the SHA-1 algorithm. An attacker could use this weakness to create forged certificate signatures. This issue affects GnuPG versions before 2.2.18.
   - Fuente: https://avd.aquasec.com/nvd/cve-2019-14855

7. Librería: libapt-pkg5.0
   - Versión: 1.8.2.3

- Id de vulnerabilidad: CVE-2011-3374
- Mensaje: It was found that apt-key in apt, all versions, do not correctly validate gpg keys with the master keyring, leading to a potential man-in-the-middle attack.
- Fuente: https://avd.aquasec.com/nvd/cve-2011-3374

8. Librería: libc-bin
   - Versión: 2.28-10
   - Id de vulnerabilidad: CVE-2010-4051
   - Mensaje: The regcomp implementation in the GNU C Library (aka glibc or libc6) through 2.11.3, and 2.12.x through 2.12.2, allows context-dependent attackers to cause a denial of service (application crash) via a regular expression containing adjacent bounded repetitions that bypass the intended RE_DUP_MAX limitation, as demonstrated by a {10,}{10,}{10,}{10,}{10,} sequence in the proftpd.gnu.c exploit for ProFTPD, related to a "RE_DUP_MAX overflow."
   - Fuente: https://avd.aquasec.com/nvd/cve-2010-4051

9. Librería: libc-bin
   - Versión: 2.28-10
   - Id de vulnerabilidad: CVE-2010-4052
   - Mensaje: Stack consumption vulnerability in the regcomp implementation in the GNU C Library (aka glibc or libc6) through 2.11.3, and 2.12.x through 2.12.2, allows context-dependent attackers to cause a denial of service (resource exhaustion) via a regular expression containing adjacent repetition operators, as demonstrated by a {10,}{10,}{10,}{10,} sequence in the proftpd.gnu.c exploit for ProFTPD.
   - Fuente: https://avd.aquasec.com/nvd/cve-2010-4052

10. Librería: libc-bin
    - Versión: 2.28-10
    - Id de vulnerabilidad: CVE-2010-4756
    - Mensaje: The glob implementation in the GNU C Library (aka glibc or libc6) allows remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in STAT commands to an FTP daemon, a different vulnerability than CVE-2010-2632.
    - Fuente: https://avd.aquasec.com/nvd/cve-2010-4756

11. Librería: libc-bin
    - Versión: 2.28-10
    - Id de vulnerabilidad: CVE-2016-10228
    - Mensaje: The iconv program in the GNU C Library (aka glibc or libc6) 2.31 and earlier,

when invoked with multiple suffixes in the destination encoding (TRANSLATE or IGNORE) along with the -c option, enters an infinite loop when processing invalid multi-byte input sequences, leading to a denial of service.

- Fuente: https://avd.aquasec.com/nvd/cve-2016-10228

12. Librería: libc-bin
    - Versión: 2.28-10
    - Id de vulnerabilidad: CVE-2018-20796
    - Mensaje: In the GNU C Library (aka glibc or libc6) through 2.29, check_dst_limits_calc_pos_1 in posix/regexec.c has Uncontrolled Recursion, as demonstrated by '(\227|)(\\1\\1|t1|\\\2537)+' in grep.
    - Fuente: https://avd.aquasec.com/nvd/cve-2018-20796

13. Librería: libc-bin
    - Versión: 2.28-10
    - Id de vulnerabilidad: CVE-2019-1010022
    - Mensaje: ** DISPUTED ** GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may bypass stack guard protection. The component is: nptl. The attack vector is: Exploit stack buffer overflow vulnerability and use this bypass vulnerability to bypass stack guard. NOTE: Upstream comments indicate "this is being treated as a non-security bug and no real threat."
    - Fuente: https://avd.aquasec.com/nvd/cve-2019-1010022

14. Librería: libc-bin
    - Versión: 2.28-10
    - Id de vulnerabilidad: CVE-2019-1010023
    - Mensaje: ** DISPUTED ** GNU Libc current is affected by: Re-mapping current loaded library with malicious ELF file. The impact is: In worst case attacker may evaluate privileges. The component is: libld. The attack vector is: Attacker sends 2 ELF files to victim and asks to run ldd on it. ldd execute code. NOTE: Upstream comments indicate "this is being treated as a non-security bug and no real threat."
    - Fuente: https://avd.aquasec.com/nvd/cve-2019-1010023

15. Librería: libc-bin
    - Versión: 2.28-10
    - Id de vulnerabilidad: CVE-2019-1010024
    - Mensaje: ** DISPUTED ** GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may bypass ASLR using cache of thread stack and heap. The component is: glibc. NOTE: Upstream comments indicate "this is being treated as a non-security bug and no real

threat."

- Fuente: https://avd.aquasec.com/nvd/cve-2019-1010024

16. Librería: libc-bin
    - Versión: 2.28-10
    - Id de vulnerabilidad: CVE-2019-1010025
    - Mensaje: ** DISPUTED ** GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may guess the heap addresses of pthread_created thread. The component is: glibc. NOTE: the vendor's position is "ASLR bypass itself is not a vulnerability."
    - Fuente: https://avd.aquasec.com/nvd/cve-2019-1010025

17. Librería: libc-bin
    - Versión: 2.28-10
    - Id de vulnerabilidad: CVE-2019-19126
    - Mensaje: On the x86-64 architecture, the GNU C Library (aka glibc) before 2.31 fails to ignore the LD_PREFER_MAP_32BIT_EXEC environment variable during program execution after a security transition, allowing local attackers to restrict the possible mapping addresses for loaded libraries and thus bypass ASLR for a setuid program.
    - Fuente: https://avd.aquasec.com/nvd/cve-2019-19126

18. Librería: libc-bin
    - Versión: 2.28-10
    - Id de vulnerabilidad: CVE-2019-9192
    - Mensaje: ** DISPUTED ** In the GNU C Library (aka glibc or libc6) through 2.29, check_dst_limits_calc_pos_1 in posix/regexec.c has Uncontrolled Recursion, as demonstrated by '(|)(\\1\\1)*' in grep, a different issue than CVE-2018-20796. NOTE: the software maintainer disputes that this is a vulnerability because the behavior occurs only with a crafted pattern.
    - Fuente: https://avd.aquasec.com/nvd/cve-2019-9192

19. Librería: libc-bin
    - Versión: 2.28-10
    - Id de vulnerabilidad: CVE-2020-6096
    - Mensaje: An exploitable signed comparison vulnerability exists in the ARMv7 memcpy() implementation of GNU glibc 2.30.9000. Calling memcpy() (on ARMv7 targets that utilize the GNU glibc implementation) with a negative value for the 'num' parameter results in a signed comparison vulnerability. If an attacker underflows the 'num' parameter to memcpy(), this vulnerability could lead to undefined behavior such as writing to out-of-bounds memory and potentially remote code execution. Furthermore, this memcpy() implementation allows for program execution to continue in

scenarios where a segmentation fault or crash should have occurred. The dangers occur in that subsequent execution and iterations of this code will be executed with this corrupted data.

- Fuente: https://avd.aquasec.com/nvd/cve-2020-6096

20. Librería: libc-bin
    - Versión: 2.28-10
    - Id de vulnerabilidad: CVE-2021-27645
    - Mensaje: The nameserver caching daemon (nscd) in the GNU C Library (aka glibc or libc6) 2.29 through 2.33, when processing a request for netgroup lookup, may crash due to a double-free, potentially resulting in degraded service or Denial of Service on the local system. This is related to netgroupcache.c.
    - Fuente: https://avd.aquasec.com/nvd/cve-2021-27645

21. Librería: libc6
    - Versión: 2.28-10
    - Id de vulnerabilidad: CVE-2010-4051
    - Mensaje: The regcomp implementation in the GNU C Library (aka glibc or libc6) through 2.11.3, and 2.12.x through 2.12.2, allows context-dependent attackers to cause a denial of service (application crash) via a regular expression containing adjacent bounded repetitions that bypass the intended RE_DUP_MAX limitation, as demonstrated by a {10,}{10,}{10,}{10,}{10,} sequence in the proftpd.gnu.c exploit for ProFTPD, related to a "RE_DUP_MAX overflow."
    - Fuente: https://avd.aquasec.com/nvd/cve-2010-4051

22. Librería: libc6
    - Versión: 2.28-10
    - Id de vulnerabilidad: CVE-2010-4052
    - Mensaje: Stack consumption vulnerability in the regcomp implementation in the GNU C Library (aka glibc or libc6) through 2.11.3, and 2.12.x through 2.12.2, allows context-dependent attackers to cause a denial of service (resource exhaustion) via a regular expression containing adjacent repetition operators, as demonstrated by a {10,}{10,}{10,}{10,} sequence in the proftpd.gnu.c exploit for ProFTPD.
    - Fuente: https://avd.aquasec.com/nvd/cve-2010-4052

23. Librería: libc6
    - Versión: 2.28-10
    - Id de vulnerabilidad: CVE-2010-4756
    - Mensaje: The glob implementation in the GNU C Library (aka glibc or libc6) allows remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob

expressions that do not match any pathnames, as demonstrated by glob expressions in STAT commands to an FTP daemon, a different vulnerability than CVE-2010-2632.

- Fuente: https://avd.aquasec.com/nvd/cve-2010-4756

24. Librería: libc6
    - Versión: 2.28-10
    - Id de vulnerabilidad: CVE-2016-10228
    - Mensaje: The iconv program in the GNU C Library (aka glibc or libc6) 2.31 and earlier, when invoked with multiple suffixes in the destination encoding (TRANSLATE or IGNORE) along with the -c option, enters an infinite loop when processing invalid multi-byte input sequences, leading to a denial of service.
    - Fuente: https://avd.aquasec.com/nvd/cve-2016-10228

25. Librería: libc6
    - Versión: 2.28-10
    - Id de vulnerabilidad: CVE-2018-20796
    - Mensaje: In the GNU C Library (aka glibc or libc6) through 2.29, check_dst_limits_calc_pos_1 in posix/regexec.c has Uncontrolled Recursion, as demonstrated by '(\227|)(\\1\\1|t1|\\\2537)+' in grep.
    - Fuente: https://avd.aquasec.com/nvd/cve-2018-20796

26. Librería: libc6
    - Versión: 2.28-10
    - Id de vulnerabilidad: CVE-2019-1010022
    - Mensaje: ** DISPUTED ** GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may bypass stack guard protection. The component is: nptl. The attack vector is: Exploit stack buffer overflow vulnerability and use this bypass vulnerability to bypass stack guard. NOTE: Upstream comments indicate "this is being treated as a non-security bug and no real threat."
    - Fuente: https://avd.aquasec.com/nvd/cve-2019-1010022

27. Librería: libc6
    - Versión: 2.28-10
    - Id de vulnerabilidad: CVE-2019-1010023
    - Mensaje: ** DISPUTED ** GNU Libc current is affected by: Re-mapping current loaded library with malicious ELF file. The impact is: In worst case attacker may evaluate privileges. The component is: libld. The attack vector is: Attacker sends 2 ELF files to victim and asks to run ldd on it. ldd execute code. NOTE: Upstream comments indicate "this is being treated as a non-security bug and no real threat."

- Fuente: https://avd.aquasec.com/nvd/cve-2019-1010023

28. Librería: libc6
    - Versión: 2.28-10
    - Id de vulnerabilidad: CVE-2019-1010024
    - Mensaje: ** DISPUTED ** GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may bypass ASLR using cache of thread stack and heap. The component is: glibc. NOTE: Upstream comments indicate "this is being treated as a non-security bug and no real threat."
    - Fuente: https://avd.aquasec.com/nvd/cve-2019-1010024

29. Librería: libc6
    - Versión: 2.28-10
    - Id de vulnerabilidad: CVE-2019-1010025
    - Mensaje: ** DISPUTED ** GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may guess the heap addresses of pthread_created thread. The component is: glibc. NOTE: the vendor's position is "ASLR bypass itself is not a vulnerability."
    - Fuente: https://avd.aquasec.com/nvd/cve-2019-1010025

30. Librería: libc6
    - Versión: 2.28-10
    - Id de vulnerabilidad: CVE-2019-19126
    - Mensaje: On the x86-64 architecture, the GNU C Library (aka glibc) before 2.31 fails to ignore the LD_PREFER_MAP_32BIT_EXEC environment variable during program execution after a security transition, allowing local attackers to restrict the possible mapping addresses for loaded libraries and thus bypass ASLR for a setuid program.
    - Fuente: https://avd.aquasec.com/nvd/cve-2019-19126

31. Librería: libc6
    - Versión: 2.28-10
    - Id de vulnerabilidad: CVE-2019-9192
    - Mensaje: ** DISPUTED ** In the GNU C Library (aka glibc or libc6) through 2.29, check_dst_limits_calc_pos_1 in posix/regexec.c has Uncontrolled Recursion, as demonstrated by '(|)(\\1\\1)*' in grep, a different issue than CVE-2018-20796. NOTE: the software maintainer disputes that this is a vulnerability because the behavior occurs only with a crafted pattern.
    - Fuente: https://avd.aquasec.com/nvd/cve-2019-9192

32. Librería: libc6

- Versión: 2.28-10
- Id de vulnerabilidad: CVE-2020-6096
- Mensaje: An exploitable signed comparison vulnerability exists in the ARMv7 memcpy() implementation of GNU glibc 2.30.9000. Calling memcpy() (on ARMv7 targets that utilize the GNU glibc implementation) with a negative value for the 'num' parameter results in a signed comparison vulnerability. If an attacker underflows the 'num' parameter to memcpy(), this vulnerability could lead to undefined behavior such as writing to out-of-bounds memory and potentially remote code execution. Furthermore, this memcpy() implementation allows for program execution to continue in scenarios where a segmentation fault or crash should have occurred. The dangers occur in that subsequent execution and iterations of this code will be executed with this corrupted data.
- Fuente: https://avd.aquasec.com/nvd/cve-2020-6096

33. Librería: libc6
    - Versión: 2.28-10
    - Id de vulnerabilidad: CVE-2021-27645
    - Mensaje: The nameserver caching daemon (nscd) in the GNU C Library (aka glibc or libc6) 2.29 through 2.33, when processing a request for netgroup lookup, may crash due to a double-free, potentially resulting in degraded service or Denial of Service on the local system. This is related to netgroupcache.c.
    - Fuente: https://avd.aquasec.com/nvd/cve-2021-27645

34. Librería: libexpat1
    - Versión: 2.2.6-2+deb10u1
    - Id de vulnerabilidad: CVE-2013-0340
    - Mensaje: expat 2.1.0 and earlier does not properly handle entities expansion unless an application developer uses the XML_SetEntityDeclHandler function, which allows remote attackers to cause a denial of service (resource consumption), send HTTP requests to intranet servers, or read arbitrary files via a crafted XML document, aka an XML External Entity (XXE) issue. NOTE: it could be argued that because expat already provides the ability to disable external entity expansion, the responsibility for resolving this issue lies with application developers; according to this argument, this entry should be REJECTed, and each affected application would need its own CVE.
    - Fuente: https://avd.aquasec.com/nvd/cve-2013-0340

35. Librería: libgcrypt20
    - Versión: 1.8.4-5
    - Id de vulnerabilidad: CVE-2018-6829
    - Mensaje: cipher/elgamal.c in Libgcrypt through 1.8.2, when used to encrypt messages

directly, improperly encodes plaintexts, which allows attackers to obtain sensitive information by reading ciphertext data (i.e., it does not have semantic security in face of a ciphertext-only attack). The Decisional Diffie-Hellman (DDH) assumption does not hold for Libgcrypt's ElGamal implementation.

- Fuente: https://avd.aquasec.com/nvd/cve-2018-6829

36. Librería: libgnutls30
    - Versión: 3.6.7-4+deb10u6
    - Id de vulnerabilidad: CVE-2011-3389
    - Mensaje: The SSL protocol, as used in certain configurations in Microsoft Windows and Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera, and other products, encrypts data by using CBC mode with chained initialization vectors, which allows man-in-the-middle attackers to obtain plaintext HTTP headers via a blockwise chosen-boundary attack (BCBA) on an HTTPS session, in conjunction with JavaScript code that uses (1) the HTML5 WebSocket API, (2) the Java URLConnection API, or (3) the Silverlight WebClient API, aka a "BEAST" attack.
    - Fuente: https://avd.aquasec.com/nvd/cve-2011-3389

37. Librería: libgssapi-krb5-2
    - Versión: 1.17-3+deb10u1
    - Id de vulnerabilidad: CVE-2004-0971
    - Mensaje: The krb5-send-pr script in the kerberos5 (krb5) package in Trustix Secure Linux 1.5 through 2.1, and possibly other operating systems, allows local users to overwrite files via a symlink attack on temporary files.
    - Fuente: https://avd.aquasec.com/nvd/cve-2004-0971

38. Librería: libgssapi-krb5-2
    - Versión: 1.17-3+deb10u1
    - Id de vulnerabilidad: CVE-2018-5709
    - Mensaje: An issue was discovered in MIT Kerberos 5 (aka krb5) through 1.16. There is a variable "dbentry->n_key_data" in kadmin/dbutil/dump.c that can store 16-bit data but unknowingly the developer has assigned a "u4" variable to it, which is for 32-bit data. An attacker can use this vulnerability to affect other artifacts of the database as we know that a Kerberos database dump file contains trusted data.
    - Fuente: https://avd.aquasec.com/nvd/cve-2018-5709

39. Librería: libjansson4
    - Versión: 2.12-1
    - Id de vulnerabilidad: CVE-2020-36325

- Mensaje: ** DISPUTED ** An issue was discovered in Jansson through 2.13.1. Due to a parsing error in json_loads, there's an out-of-bounds read-access bug. NOTE: the vendor reports that this only occurs when a programmer fails to follow the API specification.
- Fuente: https://avd.aquasec.com/nvd/cve-2020-36325

40. Librería: libk5crypto3
- Versión: 1.17-3+deb10u1
- Id de vulnerabilidad: CVE-2004-0971
- Mensaje: The krb5-send-pr script in the kerberos5 (krb5) package in Trustix Secure Linux 1.5 through 2.1, and possibly other operating systems, allows local users to overwrite files via a symlink attack on temporary files.
- Fuente: https://avd.aquasec.com/nvd/cve-2004-0971

41. Librería: libk5crypto3
- Versión: 1.17-3+deb10u1
- Id de vulnerabilidad: CVE-2018-5709
- Mensaje: An issue was discovered in MIT Kerberos 5 (aka krb5) through 1.16. There is a variable "dbentry->n_key_data" in kadmin/dbutil/dump.c that can store 16-bit data but unknowingly the developer has assigned a "u4" variable to it, which is for 32-bit data. An attacker can use this vulnerability to affect other artifacts of the database as we know that a Kerberos database dump file contains trusted data.
- Fuente: https://avd.aquasec.com/nvd/cve-2018-5709

42. Librería: libkrb5-3
- Versión: 1.17-3+deb10u1
- Id de vulnerabilidad: CVE-2004-0971
- Mensaje: The krb5-send-pr script in the kerberos5 (krb5) package in Trustix Secure Linux 1.5 through 2.1, and possibly other operating systems, allows local users to overwrite files via a symlink attack on temporary files.
- Fuente: https://avd.aquasec.com/nvd/cve-2004-0971

43. Librería: libkrb5-3
- Versión: 1.17-3+deb10u1
- Id de vulnerabilidad: CVE-2018-5709
- Mensaje: An issue was discovered in MIT Kerberos 5 (aka krb5) through 1.16. There is a variable "dbentry->n_key_data" in kadmin/dbutil/dump.c that can store 16-bit data but unknowingly the developer has assigned a "u4" variable to it, which is for 32-bit data. An attacker can use this vulnerability to affect other artifacts of the database as we know that a Kerberos database dump

file contains trusted data.

- Fuente: https://avd.aquasec.com/nvd/cve-2018-5709

44. Librería: libkrb5support0
    - Versión: 1.17-3+deb10u1
    - Id de vulnerabilidad: CVE-2004-0971
    - Mensaje: The krb5-send-pr script in the kerberos5 (krb5) package in Trustix Secure Linux 1.5 through 2.1, and possibly other operating systems, allows local users to overwrite files via a symlink attack on temporary files.
    - Fuente: https://avd.aquasec.com/nvd/cve-2004-0971

45. Librería: libkrb5support0
    - Versión: 1.17-3+deb10u1
    - Id de vulnerabilidad: CVE-2018-5709
    - Mensaje: An issue was discovered in MIT Kerberos 5 (aka krb5) through 1.16. There is a variable "dbentry->n_key_data" in kadmin/dbutil/dump.c that can store 16-bit data but unknowingly the developer has assigned a "u4" variable to it, which is for 32-bit data. An attacker can use this vulnerability to affect other artifacts of the database as we know that a Kerberos database dump file contains trusted data.
    - Fuente: https://avd.aquasec.com/nvd/cve-2018-5709

46. Librería: libldap-2.4-2
    - Versión: 2.4.47+dfsg-3+deb10u6
    - Id de vulnerabilidad: CVE-2015-3276
    - Mensaje: The nss_parse_ciphers function in libraries/libldap/tls_m.c in OpenLDAP does not properly parse OpenSSL-style multi-keyword mode cipher strings, which might cause a weaker than intended cipher to be used and allow remote attackers to have unspecified impact via unknown vectors.
    - Fuente: https://avd.aquasec.com/nvd/cve-2015-3276

47. Librería: libldap-2.4-2
    - Versión: 2.4.47+dfsg-3+deb10u6
    - Id de vulnerabilidad: CVE-2017-14159
    - Mensaje: slapd in OpenLDAP 2.4.45 and earlier creates a PID file after dropping privileges to a non-root account, which might allow local users to kill arbitrary processes by leveraging access to this non-root account for PID file modification before a root script executes a "kill `cat /pathname`" command, as demonstrated by openldap-initscript.
    - Fuente: https://avd.aquasec.com/nvd/cve-2017-14159

48. Librería: libldap-2.4-2
    - Versión: 2.4.47+dfsg-3+deb10u6
    - Id de vulnerabilidad: CVE-2017-17740
    - Mensaje: contrib/slapd-modules/nops/nops.c in OpenLDAP through 2.4.45, when both the nops module and the memberof overlay are enabled, attempts to free a buffer that was allocated on the stack, which allows remote attackers to cause a denial of service (slapd crash) via a member MODDN operation.
    - Fuente: https://avd.aquasec.com/nvd/cve-2017-17740

49. Librería: libldap-2.4-2
    - Versión: 2.4.47+dfsg-3+deb10u6
    - Id de vulnerabilidad: CVE-2020-15719
    - Mensaje: libldap in certain third-party OpenLDAP packages has a certificate-validation flaw when the third-party package is asserting RFC6125 support. It considers CN even when there is a non-matching subjectAltName (SAN). This is fixed in, for example, openldap-2.4.46-10.el8 in Red Hat Enterprise Linux.
    - Fuente: https://avd.aquasec.com/nvd/cve-2020-15719

50. Librería: libldap-common
    - Versión: 2.4.47+dfsg-3+deb10u6
    - Id de vulnerabilidad: CVE-2015-3276
    - Mensaje: The nss_parse_ciphers function in libraries/libldap/tls_m.c in OpenLDAP does not properly parse OpenSSL-style multi-keyword mode cipher strings, which might cause a weaker than intended cipher to be used and allow remote attackers to have unspecified impact via unknown vectors.
    - Fuente: https://avd.aquasec.com/nvd/cve-2015-3276

51. Librería: libldap-common
    - Versión: 2.4.47+dfsg-3+deb10u6
    - Id de vulnerabilidad: CVE-2017-14159
    - Mensaje: slapd in OpenLDAP 2.4.45 and earlier creates a PID file after dropping privileges to a non-root account, which might allow local users to kill arbitrary processes by leveraging access to this non-root account for PID file modification before a root script executes a "kill `cat /pathname`" command, as demonstrated by openldap-initscript.
    - Fuente: https://avd.aquasec.com/nvd/cve-2017-14159

52. Librería: libldap-common

- Versión: 2.4.47+dfsg-3+deb10u6
- Id de vulnerabilidad: CVE-2017-17740
- Mensaje: contrib/slapd-modules/nops/nops.c in OpenLDAP through 2.4.45, when both the nops module and the memberof overlay are enabled, attempts to free a buffer that was allocated on the stack, which allows remote attackers to cause a denial of service (slapd crash) via a member MODDN operation.
- Fuente: https://avd.aquasec.com/nvd/cve-2017-17740

53. Librería: libldap-common
- Versión: 2.4.47+dfsg-3+deb10u6
- Id de vulnerabilidad: CVE-2020-15719
- Mensaje: libldap in certain third-party OpenLDAP packages has a certificate-validation flaw when the third-party package is asserting RFC6125 support. It considers CN even when there is a non-matching subjectAltName (SAN). This is fixed in, for example, openldap-2.4.46-10.el8 in Red Hat Enterprise Linux.
- Fuente: https://avd.aquasec.com/nvd/cve-2020-15719

54. Librería: liblz4-1
- Versión: 1.8.3-1
- Id de vulnerabilidad: CVE-2019-17543
- Mensaje: LZ4 before 1.9.2 has a heap-based buffer overflow in LZ4_write32 (related to LZ4_compress_destSize), affecting applications that call LZ4_compress_fast with a large input. (This issue can also lead to data corruption.) NOTE: the vendor states "only a few specific / uncommon usages of the API are at risk."
- Fuente: https://avd.aquasec.com/nvd/cve-2019-17543

55. Librería: libnghttp2-14
- Versión: 1.36.0-2+deb10u1
- Id de vulnerabilidad: TEMP-0000000-A4EF31
- Mensaje: null
- Fuente: https://security-tracker.debian.org/tracker/TEMP-0000000-A4EF31

56. Librería: libpcre3
- Versión: 2:8.39-12
- Id de vulnerabilidad: CVE-2017-11164
- Mensaje: In PCRE 8.41, the OP_KETRMAX feature in the match function in pcre_exec.c allows stack exhaustion (uncontrolled recursion) when processing a crafted regular expression.
- Fuente: https://avd.aquasec.com/nvd/cve-2017-11164

57. Librería: libpcre3
- Versión: 2:8.39-12
- Id de vulnerabilidad: CVE-2017-16231
- Mensaje: ** DISPUTED ** In PCRE 8.41, after compiling, a pcretest load test PoC produces a crash overflow in the function match() in pcre_exec.c because of a self-recursive call. NOTE: third parties dispute the relevance of this report, noting that there are options that can be used to limit the amount of stack that is used.
- Fuente: https://avd.aquasec.com/nvd/cve-2017-16231

58. Librería: libpcre3
- Versión: 2:8.39-12
- Id de vulnerabilidad: CVE-2017-7245
- Mensaje: Stack-based buffer overflow in the pcre32_copy_substring function in pcre_get.c in libpcre1 in PCRE 8.40 allows remote attackers to cause a denial of service (WRITE of size 4) or possibly have unspecified other impact via a crafted file.
- Fuente: https://avd.aquasec.com/nvd/cve-2017-7245

59. Librería: libpcre3
- Versión: 2:8.39-12
- Id de vulnerabilidad: CVE-2017-7246
- Mensaje: Stack-based buffer overflow in the pcre32_copy_substring function in pcre_get.c in libpcre1 in PCRE 8.40 allows remote attackers to cause a denial of service (WRITE of size 268) or possibly have unspecified other impact via a crafted file.
- Fuente: https://avd.aquasec.com/nvd/cve-2017-7246

60. Librería: libpcre3
- Versión: 2:8.39-12
- Id de vulnerabilidad: CVE-2019-20838
- Mensaje: libpcre in PCRE before 8.43 allows a subject buffer over-read in JIT when UTF is disabled, and \X or \R has more than one fixed quantifier, a related issue to CVE-2019-20454.
- Fuente: https://avd.aquasec.com/nvd/cve-2019-20838

61. Librería: libseccomp2
- Versión: 2.3.3-4
- Id de vulnerabilidad: CVE-2019-9893
- Mensaje: libseccomp before 2.4.0 did not correctly generate 64-bit syscall argument comparisons using the arithmetic operators (LT, GT, LE, GE), which might able to lead to

bypassing seccomp filters and potential privilege escalations.
- Fuente: https://avd.aquasec.com/nvd/cve-2019-9893

62. Librería: libssh2-1
- Versión: 1.8.0-2.1
- Id de vulnerabilidad: CVE-2019-17498
- Mensaje: In libssh2 v1.9.0 and earlier versions, the SSH_MSG_DISCONNECT logic in packet.c has an integer overflow in a bounds check, enabling an attacker to specify an arbitrary (out-of-bounds) offset for a subsequent memory read. A crafted SSH server may be able to disclose sensitive information or cause a denial of service condition on the client system when a user connects to the server.
- Fuente: https://avd.aquasec.com/nvd/cve-2019-17498

63. Librería: libssl1.1
- Versión: 1.1.1d-0+deb10u6
- Id de vulnerabilidad: CVE-2007-6755
- Mensaje: The NIST SP 800-90A default statement of the Dual Elliptic Curve Deterministic Random Bit Generation (Dual_EC_DRBG) algorithm contains point Q constants with a possible relationship to certain "skeleton key" values, which might allow context-dependent attackers to defeat cryptographic protection mechanisms by leveraging knowledge of those values. NOTE: this is a preliminary CVE for Dual_EC_DRBG; future research may provide additional details about point Q and associated attacks, and could potentially lead to a RECAST or REJECT of this CVE.
- Fuente: https://avd.aquasec.com/nvd/cve-2007-6755

64. Librería: libssl1.1
- Versión: 1.1.1d-0+deb10u6
- Id de vulnerabilidad: CVE-2010-0928
- Mensaje: OpenSSL 0.9.8i on the Gaisler Research LEON3 SoC on the Xilinx Virtex-II Pro FPGA uses a Fixed Width Exponentiation (FWE) algorithm for certain signature calculations, and does not verify the signature before providing it to a caller, which makes it easier for physically proximate attackers to determine the private key via a modified supply voltage for the microprocessor, related to a "fault-based attack."
- Fuente: https://avd.aquasec.com/nvd/cve-2010-0928

65. Librería: libsystemd0
- Versión: 241-7~deb10u7
- Id de vulnerabilidad: CVE-2013-4392
- Mensaje: systemd, when updating file permissions, allows local users to change the

permissions and SELinux security contexts for arbitrary files via a symlink attack on unspecified files.

- Fuente: https://avd.aquasec.com/nvd/cve-2013-4392

66. Librería: libsystemd0
    - Versión: 241-7~deb10u7
    - Id de vulnerabilidad: CVE-2019-20386
    - Mensaje: An issue was discovered in button_open in login/logind-button.c in systemd before 243. When executing the udevadm trigger command, a memory leak may occur.
    - Fuente: https://avd.aquasec.com/nvd/cve-2019-20386

67. Librería: libsystemd0
    - Versión: 241-7~deb10u7
    - Id de vulnerabilidad: CVE-2020-13529
    - Mensaje: An exploitable denial-of-service vulnerability exists in Systemd 245. A specially crafted DHCP FORCERENEW packet can cause a server running the DHCP client to be vulnerable to a DHCP ACK spoofing attack. An attacker can forge a pair of FORCERENEW and DCHP ACK packets to reconfigure the server.
    - Fuente: https://avd.aquasec.com/nvd/cve-2020-13529

68. Librería: libsystemd0
    - Versión: 241-7~deb10u7
    - Id de vulnerabilidad: CVE-2020-13776
    - Mensaje: systemd through v245 mishandles numerical usernames such as ones composed of decimal digits or 0x followed by hex digits, as demonstrated by use of root privileges when privileges of the 0x0 user account were intended. NOTE: this issue exists because of an incomplete fix for CVE-2017-1000082.
    - Fuente: https://avd.aquasec.com/nvd/cve-2020-13776

69. Librería: libtasn1-6
    - Versión: 4.13-3
    - Id de vulnerabilidad: CVE-2018-1000654
    - Mensaje: GNU Libtasn1-4.13 libtasn1-4.13 version libtasn1-4.13, libtasn1-4.12 contains a DoS, specifically CPU usage will reach 100% when running asn1Paser against the POC due to an issue in _asn1_expand_object_id(p_tree), after a long time, the program will be killed. This attack appears to be exploitable via parsing a crafted file.
    - Fuente: https://avd.aquasec.com/nvd/cve-2018-1000654

70. Librería: libudev1
- Versión: 241-7~deb10u7
- Id de vulnerabilidad: CVE-2013-4392
- Mensaje: systemd, when updating file permissions, allows local users to change the permissions and SELinux security contexts for arbitrary files via a symlink attack on unspecified files.
- Fuente: https://avd.aquasec.com/nvd/cve-2013-4392

71. Librería: libudev1
- Versión: 241-7~deb10u7
- Id de vulnerabilidad: CVE-2019-20386
- Mensaje: An issue was discovered in button_open in login/logind-button.c in systemd before 243. When executing the udevadm trigger command, a memory leak may occur.
- Fuente: https://avd.aquasec.com/nvd/cve-2019-20386

72. Librería: libudev1
- Versión: 241-7~deb10u7
- Id de vulnerabilidad: CVE-2020-13529
- Mensaje: An exploitable denial-of-service vulnerability exists in Systemd 245. A specially crafted DHCP FORCERENEW packet can cause a server running the DHCP client to be vulnerable to a DHCP ACK spoofing attack. An attacker can forge a pair of FORCERENEW and DCHP ACK packets to reconfigure the server.
- Fuente: https://avd.aquasec.com/nvd/cve-2020-13529

73. Librería: libudev1
- Versión: 241-7~deb10u7
- Id de vulnerabilidad: CVE-2020-13776
- Mensaje: systemd through v245 mishandles numerical usernames such as ones composed of decimal digits or 0x followed by hex digits, as demonstrated by use of root privileges when privileges of the 0x0 user account were intended. NOTE: this issue exists because of an incomplete fix for CVE-2017-1000082.
- Fuente: https://avd.aquasec.com/nvd/cve-2020-13776

74. Librería: libxml2
- Versión: 2.9.4+dfsg1-7+deb10u1
- Id de vulnerabilidad: CVE-2020-24977
- Mensaje: GNOME project libxml2 v2.9.10 has a global buffer over-read vulnerability in xmlEncodeEntitiesInternal at libxml2/entities.c. The issue has been fixed in commit 50f06b3e.

- Fuente: https://avd.aquasec.com/nvd/cve-2020-24977

75. Librería: login
    - Versión: 1:4.5-1.1
    - Id de vulnerabilidad: CVE-2007-5686
    - Mensaje: initscripts in rPath Linux 1 sets insecure permissions for the /var/log/btmp file, which allows local users to obtain sensitive information regarding authentication attempts. NOTE: because sshd detects the insecure permissions and does not log certain events, this also prevents sshd from logging failed authentication attempts by remote attackers.
    - Fuente: https://avd.aquasec.com/nvd/cve-2007-5686

76. Librería: login
    - Versión: 1:4.5-1.1
    - Id de vulnerabilidad: CVE-2013-4235
    - Mensaje: shadow: TOCTOU (time-of-check time-of-use) race condition when copying and removing directory trees
    - Fuente: https://avd.aquasec.com/nvd/cve-2013-4235

77. Librería: login
    - Versión: 1:4.5-1.1
    - Id de vulnerabilidad: CVE-2018-7169
    - Mensaje: An issue was discovered in shadow 4.5. newgidmap (in shadow-utils) is setuid and allows an unprivileged user to be placed in a user namespace where setgroups(2) is permitted. This allows an attacker to remove themselves from a supplementary group, which may allow access to certain filesystem paths if the administrator has used "group blacklisting" (e.g., chmod g-rwx) to restrict access to paths. This flaw effectively reverts a security feature in the kernel (in particular, the /proc/self/setgroups knob) to prevent this sort of privilege escalation.
    - Fuente: https://avd.aquasec.com/nvd/cve-2018-7169

78. Librería: login
    - Versión: 1:4.5-1.1
    - Id de vulnerabilidad: CVE-2019-19882
    - Mensaje: shadow 4.8, in certain circumstances affecting at least Gentoo, Arch Linux, and Void Linux, allows local users to obtain root access because setuid programs are misconfigured. Specifically, this affects shadow 4.8 when compiled using --with-libpam but without explicitly passing --disable-account-tools-setuid, and without a PAM configuration suitable for use with setuid account management tools. This combination leads to account management tools (groupadd, groupdel, groupmod, useradd, userdel, usermod) that can easily be used by

unprivileged local users to escalate privileges to root in multiple ways. This issue became much more relevant in approximately December 2019 when an unrelated bug was fixed (i.e., the chmod calls to suidusbins were fixed in the upstream Makefile which is now included in the release version 4.8).

- Fuente: https://avd.aquasec.com/nvd/cve-2019-19882

79. Librería: login
    - Versión: 1:4.5-1.1
    - Id de vulnerabilidad: TEMP-0628843-DBAD28
    - Mensaje: null
    - Fuente: https://security-tracker.debian.org/tracker/TEMP-0628843-DBAD28

80. Librería: passwd
    - Versión: 1:4.5-1.1
    - Id de vulnerabilidad: CVE-2007-5686
    - Mensaje: initscripts in rPath Linux 1 sets insecure permissions for the /var/log/btmp file, which allows local users to obtain sensitive information regarding authentication attempts. NOTE: because sshd detects the insecure permissions and does not log certain events, this also prevents sshd from logging failed authentication attempts by remote attackers.
    - Fuente: https://avd.aquasec.com/nvd/cve-2007-5686

81. Librería: passwd
    - Versión: 1:4.5-1.1
    - Id de vulnerabilidad: CVE-2013-4235
    - Mensaje: shadow: TOCTOU (time-of-check time-of-use) race condition when copying and removing directory trees
    - Fuente: https://avd.aquasec.com/nvd/cve-2013-4235

82. Librería: passwd
    - Versión: 1:4.5-1.1
    - Id de vulnerabilidad: CVE-2018-7169
    - Mensaje: An issue was discovered in shadow 4.5. newgidmap (in shadow-utils) is setuid and allows an unprivileged user to be placed in a user namespace where setgroups(2) is permitted. This allows an attacker to remove themselves from a supplementary group, which may allow access to certain filesystem paths if the administrator has used "group blacklisting" (e.g., chmod g-rwx) to restrict access to paths. This flaw effectively reverts a security feature in the kernel (in particular, the /proc/self/setgroups knob) to prevent this sort of privilege escalation.
    - Fuente: https://avd.aquasec.com/nvd/cve-2018-7169

83. Librería: passwd
    - Versión: 1:4.5-1.1
    - Id de vulnerabilidad: CVE-2019-19882
    - Mensaje: shadow 4.8, in certain circumstances affecting at least Gentoo, Arch Linux, and Void Linux, allows local users to obtain root access because setuid programs are misconfigured. Specifically, this affects shadow 4.8 when compiled using --with-libpam but without explicitly passing --disable-account-tools-setuid, and without a PAM configuration suitable for use with setuid account management tools. This combination leads to account management tools (groupadd, groupdel, groupmod, useradd, userdel, usermod) that can easily be used by unprivileged local users to escalate privileges to root in multiple ways. This issue became much more relevant in approximately December 2019 when an unrelated bug was fixed (i.e., the chmod calls to suidusbins were fixed in the upstream Makefile which is now included in the release version 4.8).
    - Fuente: https://avd.aquasec.com/nvd/cve-2019-19882

84. Librería: passwd
    - Versión: 1:4.5-1.1
    - Id de vulnerabilidad: TEMP-0628843-DBAD28
    - Mensaje: null
    - Fuente: https://security-tracker.debian.org/tracker/TEMP-0628843-DBAD28

85. Librería: perl-base
    - Versión: 5.28.1-6+deb10u1
    - Id de vulnerabilidad: CVE-2011-4116
    - Mensaje: _is_safe in the File::Temp module for Perl does not properly handle symlinks.
    - Fuente: https://avd.aquasec.com/nvd/cve-2011-4116

86. Librería: sysvinit-utils
    - Versión: 2.93-8
    - Id de vulnerabilidad: TEMP-0517018-A83CE6
    - Mensaje: null
    - Fuente: https://security-tracker.debian.org/tracker/TEMP-0517018-A83CE6

87. Librería: tar
    - Versión: 1.30+dfsg-6
    - Id de vulnerabilidad: CVE-2005-2541
    - Mensaje: Tar 1.15.1 does not properly warn the user when extracting setuid or setgid files,

which may allow local users or remote attackers to gain privileges.

- Fuente: https://avd.aquasec.com/nvd/cve-2005-2541

88. Librería: tar
    - Versión: 1.30+dfsg-6
    - Id de vulnerabilidad: CVE-2019-9923
    - Mensaje: pax_decode_header in sparse.c in GNU Tar before 1.32 had a NULL pointer dereference when parsing certain archives that have malformed extended headers.
    - Fuente: https://avd.aquasec.com/nvd/cve-2019-9923

89. Librería: tar
    - Versión: 1.30+dfsg-6
    - Id de vulnerabilidad: CVE-2021-20193
    - Mensaje: A flaw was found in the src/list.c of tar 1.33 and earlier. This flaw allows an attacker who can submit a crafted input file to tar to cause uncontrolled consumption of memory. The highest threat from this vulnerability is to system availability.
    - Fuente: https://avd.aquasec.com/nvd/cve-2021-20193

90. Librería: tar
    - Versión: 1.30+dfsg-6
    - Id de vulnerabilidad: TEMP-0290435-0B57B5
    - Mensaje: null
    - Fuente: https://security-tracker.debian.org/tracker/TEMP-0290435-0B57B5

5.1.3 Rapidscan.

Rapidscan	
Severidad	**Cantidad**
Críticas	1
Altas	3
Medias	4
Bajas	3
Información	0

Detalle de vulnerabilidades de tipo: Críticas

1. Clasificacion: XSSer found XSS vulnerabilities.

- Vulnerabilidad: An attacker will be able to steal cookies, deface web application or redirect to any third party address that can serve malware.

- Recomendación: Input validation and Output Sanitization can completely prevent Cross Site Scripting (XSS) attacks. XSS attacks can be mitigated in future by properly following a secure coding methodology. The following comprehensive resource provides detailed information on fixing this vulnerability. https

Detalle de vulnerabilidades de tipo: Altas

1. Clasificacion: Uniscan detected possible XSS, SQLi, BSQLi.

- Vulnerabilidad: Hackers will be able to steal data from the backend and also they can authenticate themselves to the website and can impersonate as any user since they have total control over the backend. They can even wipe out the entire database. Attackers can also steal cookie information of an authenticated user and they can even redirect the target to any malicious address or totally deface the application.

- Recomendación: Proper input validation has to be done prior to directly querying the database information. A developer should remember not to trust an end-user's input. By following a secure coding methodology attacks like SQLi, XSS and BSQLi. The following resource guides on how to implement secure coding methodology on application development. https

2. Clasificacion: Domain is spoofed/hijacked.

- Vulnerabilidad: An attacker can forwarded requests that comes to the legitimate URL or web application to a third party address or to the attacker's location that can serve malware and affect

the end user's machine.

- Recomendación: It is highly recommended to deploy DNSSec on the host target. Full deployment of DNSSEC will ensure the end user is connecting to the actual web site or other service corresponding to a particular domain name. For more information, check this resource. https

3. Clasificacion: HEARTBLEED Vulnerability Found with Golismero.

- Vulnerabilidad: This vulnerability seriously leaks private information of your host. An attacker can keep the TLS connection alive and can retrieve a maximum of 64K of data per heartbeat.

- Recomendación: PFS (Perfect Forward Secrecy) can be implemented to make decryption difficult. Complete remediation and resource information is available here. http

Detalle de vulnerabilidades de tipo: Medias

1. Clasificacion: Open Directories Found with Golismero BruteForce.

- Vulnerabilidad: Attackers may find considerable amount of information from these directories. There are even chances attackers may get access to critical information from these directories.

- Recomendación: It is recommended to block or restrict access to these directories unless necessary.

2. Clasificacion: X-XSS Protection is not Present

- Vulnerabilidad: As the target is lacking this header, older browsers will be prone to Reflected XSS attacks.

- Recomendación: Modern browsers does not face any issues with this vulnerability (missing headers). However, older browsers are strongly recommended to be upgraded.

3. Clasificacion: Open Files Found with Golismero BruteForce.

- Vulnerabilidad: Attackers may find considerable amount of information from these files. There are even chances attackers may get access to critical information from these files.

- Recomendación: It is recommended to block or restrict access to these files unless necessary.

4. Clasificacion: Golismero Nikto Plugin found vulnerabilities.

- Vulnerabilidad: Particular Scanner found multiple vulnerabilities that an attacker may try to exploit the target.

- Recomendación: Refer to RS-Vulnerability-Report to view the complete information of the

vulnerability, once the scan gets completed.

Detalle de vulnerabilidades de tipo: Bajas

1. Clasificacion: No DNS/HTTP based Load Balancers Found.

- Vulnerabilidad: This has nothing to do with security risks, however attackers may use this unavailability of load balancers as an advantage to leverage a denial of service attack on certain services or on the whole application itself.

- Recomendación: Load-Balancers are highly encouraged for any web application. They improve performance times as well as data availability on during times of server outage. To know more information on load balancers and setup, check this resource. https

2. Clasificacion: Found some information through Fingerprinting.

- Vulnerabilidad: Attackers always do a fingerprint of any server before they launch an attack. Fingerprinting gives them information about the server type, content- they are serving, last modification times etc, this gives an attacker to learn more information about the target

- Recomendación: A good practice is to obfuscate the information to outside world. Doing so, the attackers will have tough time understanding the server's tech stack and therefore leverage an attack.

3. Clasificacion: DB Banner retrieved with SQLMap.

- Vulnerabilidad: May not be SQLi vulnerable. An attacker will be able to know that the host is using a backend for operation.

- Recomendación: Banner Grabbing should be restricted and access to the services from outside would should be made minimum.