

Informe Ejecutivo de Vulnerabilidades

Generado en: 2026-09-03T13:24:48.215Z | Fuentes: ENISA

- Informes consolidados: 10
- Vulnerabilidades analizadas: 206
- Aplicables: 28
- No aplicables: 178
- Revisión manual: 0

Resumen por objetivo

Fuente	Producto	Versión	Analizadas	Aplicables	No aplicables	Revisión manual	Necesidad Parcheo
ENISA	Tomcat	9.0.119	20	0	20	0	Sin Acción
ENISA	Tomcat	11.0.23	20	0	20	0	Sin Acción
ENISA	Jenkins	2.568.1	92	18	74	0	Diferible
ENISA	Harbor	2.11.0	0	0	0	0	Sin Acción
ENISA	Openjdk	21.0.12	2	0	2	0	Sin Acción
ENISA	Openjdk	1.8.0.502	2	2	0	0	Diferible
ENISA	GitLab CE	19.2.4	66	7	59	0	Diferible
ENISA	Nginx	1.30.3	1	0	1	0	Sin Acción
ENISA	Artemis	2.54.0	2	0	2	0	Sin Acción
ENISA	JasperReports	10.0.0	1	1	0	0	Diferible

Detalle de Vulnerabilidades Aplicables

[CRÍTICA] - EUVD-2026-55694 - GHSA-p2q7-r6vq-359j

- **Producto / Versión:** JasperReports (v10.0.0) | **Fuente:** ENISA
- **BaseScore:** 9.3 4.0 | **Parcheo Vulnerabilidad:** Diferible
- **Vector CVSS:** CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:L/SC:L/SI:L/SA:L
- **Regla versión:** product_version: “10.0.0 <HF-10” -> (Cumple condiciones: Rama/Coincidencia 10.0.0 (Sí))
- **Justificación / Descripción:** > Improper restriction of XML external entity reference vulnerability (unauthenticated) in Jaspersoft JasperReports Server.

This issue affects JasperReports Server: from 9.0.0 befor...

[CRÍTICA] - EUVD-2026-53569 - GHSA-v269-8r2r-vj93

- **Producto / Versión:** Jenkins (v2.568.1) | **Fuente:** ENISA
- **BaseScore:** 9.0 3.1 | **Parcheo Vulnerabilidad:** Diferible
- **Vector CVSS:** CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H
- **Regla versión:** product_version: “patch: 3355.3357.v931d3c992987” -> (2.568.1 anterior al parche 3355.3357)
- **Justificación / Descripción:** > In Remoting 3384.v60d89463d9e0 and earlier, except 3355.3357.v931d3c992987, included in Jenkins 2.575 and earlier, LTS 2.568.1 and earlier, the JEP-200 class filter is not applied...

[ALTA] - EUVD-2026-70111 - GHSA-g5fg-fmcm-8xx6

- **Producto / Versión:** Jenkins (v2.568.1) | **Fuente:** ENISA
- **BaseScore:** 8.8 3.1 | **Parcheo Vulnerabilidad:** Diferible
- **Vector CVSS:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
- **Regla versión:** product_version: “patch: 2.568.3” -> (2.568.1 anterior al parche 2.568.3)

- **Justificación / Descripción:** > In Jenkins 2.579 and earlier, LTS 2.568.2 and earlier, objects of types marked as storing their configuration in independent top-level configuration files in Jenkins (such as the g...
-

[ALTA] - EUVD-2026-70113 - CVE-2026-84647

- **Producto / Versión:** Jenkins (v2.568.1) | **Fuente:** ENISA
 - **BaseScore:** 8.8 3.1 | **Parcheo Vulnerabilidad:** Diferible
 - **Vector CVSS:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
 - **Regla versión:** product_version: "patch: 2.580" -> (2.568.1 anterior al parche 2.580)
 - **Justificación / Descripción:** > In Stapler 2107.v8dfcb_e8ed317 and earlier, except 2088.2093.vd7c3e58008a_6, included in Jenkins 2.579 and earlier, LTS 2.568.2 and earlier, Stapler does not restrict the types of...
-

[ALTA] - EUVD-2026-70114 - CVE-2026-84648

- **Producto / Versión:** Jenkins (v2.568.1) | **Fuente:** ENISA
 - **BaseScore:** 8.8 3.1 | **Parcheo Vulnerabilidad:** Diferible
 - **Vector CVSS:** CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
 - **Regla versión:** product_version: "patch: 2.580" -> (2.568.1 anterior al parche 2.580)
 - **Justificación / Descripción:** > In Jenkins 2.579 and earlier, LTS 2.568.2 and earlier, the system log viewer does not escape log record metadata (source, level, and timestamp) resulting in a stored cross-site scr...
-

[ALTA] - EUVD-2026-70115 - CVE-2026-84649

- **Producto / Versión:** Jenkins (v2.568.1) | **Fuente:** ENISA
 - **BaseScore:** 8.8 3.1 | **Parcheo Vulnerabilidad:** Diferible
 - **Vector CVSS:** CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
 - **Regla versión:** product_version: "patch: 2.568.3" -> (2.568.1 anterior al parche 2.568.3)
 - **Justificación / Descripción:** > In Stapler 1839.ved17667b_a_eb_5 through 2107.v8dfcb_e8ed317 (both inclusive), except 2088.2093.vd7c3e58008a_6, included in Jenkins 2.447 through 2.579 (both inclusive), LTS 2.452....
-

[ALTA] - EUVD-2026-70116 - CVE-2026-84650

- **Producto / Versión:** Jenkins (v2.568.1) | **Fuente:** ENISA
 - **BaseScore:** 8.8 3.1 | **Parcheo Vulnerabilidad:** Diferible
 - **Vector CVSS:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
 - **Regla versión:** product_version: "patch: 2.580" -> (2.568.1 anterior al parche 2.580)
 - **Justificación / Descripción:** > In Jenkins 2.579 and earlier, LTS 2.568.2 and earlier, transient fields cannot be excluded from deserialization, allowing attackers able to submit configuration updates to specify...
-

[ALTA] - EUVD-2026-42435 - GHSA-xg8h-3f4m-39v6

- **Producto / Versión:** Openjdk (v1.8.0.502) | **Fuente:** ENISA
 - **BaseScore:** 8.8 3.1 | **Parcheo Vulnerabilidad:** Descartable
 - **Vector CVSS:** CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
 - **Regla versión:** product_version: "0 <3.74ubuntu1.1" -> (Cumple condiciones: 1.8.0.502 < 3.74 (Sí))
 - **Justificación / Descripción:** > A sandbox escape vulnerability exists in the OpenJDK packages provided in Ubuntu. The .jar MIME handlers installed by these packages execute files marked as executable when the mai...
-

[ALTA] - EUVD-2026-53523 - GHSA-7fgq-gph8-29q5

- **Producto / Versión:** Jenkins (v2.568.1) | **Fuente:** ENISA
 - **BaseScore:** 8.1 3.1 | **Parcheo Vulnerabilidad:** Diferible
 - **Vector CVSS:** CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
 - **Regla versión:** product_version: “patch: 2.568.2” -> (2.568.1 anterior al parche 2.568.2)
 - **Justificación / Descripción:** > Jenkins 2.575 and earlier, LTS 2.568.1 and earlier handles case-insensitivity in user names and group names inconsistently, allowing attackers able to create new users or groups wi...
-

[ALTA] - EUVD-2026-55984 - CVE-2026-15560

- **Producto / Versión:** Openjdk (v1.8.0.502) | **Fuente:** ENISA
 - **BaseScore:** 8.1 3.1 | **Parcheo Vulnerabilidad:** Diferible
 - **Vector CVSS:** CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
 - **Regla versión:** product_version: “patch: 0:2.3.14-11.SP11_redhat_00001.1.el7eap” -> (1.8.0.502 anterior al parche 2.3.14)
 - **Justificación / Descripción:** > when EAP runs with -secmgr, the openjdk-orb’s JDKBridge honours attacker-supplied CDR codebase URLs during object unmarshalling on :3528, allowing an unauthenticated attacker to lo...
-

[ALTA] - EUVD-2026-66428 - GHSA-gjcp-3p8v-jvrw

- **Producto / Versión:** GitLab CE (v19.2.4) | **Fuente:** ENISA
 - **BaseScore:** 7.3 3.1 | **Parcheo Vulnerabilidad:** Diferible
 - **Vector CVSS:** CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N
 - **Regla versión:** product_version: “19.2 <19.2.5” -> (Cumple condiciones: Rama/Coincidencia 19.2 (Sí) | 19.2.4 < 19.2.5 (Sí))
 - **Justificación / Descripción:** > GitLab has remediated an issue in GitLab EE affecting all versions from 18.9 before 19.1.7, 19.2 before 19.2.5, and 19.3 before 19.3.1 that, under certain conditions, an authentica...
-

[MEDIA] - EUVD-2026-66427 - CVE-2026-77801

- **Producto / Versión:** GitLab CE (v19.2.4) | **Fuente:** ENISA
 - **BaseScore:** 6.5 3.1 | **Parcheo Vulnerabilidad:** Diferible
 - **Vector CVSS:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
 - **Regla versión:** product_version: “19.2 <19.2.5” -> (Cumple condiciones: Rama/Coincidencia 19.2 (Sí) | 19.2.4 < 19.2.5 (Sí))
 - **Justificación / Descripción:** > GitLab has remediated an issue in GitLab CE/EE affecting all versions from 12.8 before 19.1.7, 19.2 before 19.2.5, and 19.3 before 19.3.1 that, under certain conditions, could have...
-

[MEDIA] - EUVD-2025-210778 - CVE-2025-10903

- **Producto / Versión:** GitLab CE (v19.2.4) | **Fuente:** ENISA
 - **BaseScore:** 6.5 3.1 | **Parcheo Vulnerabilidad:** Diferible
 - **Vector CVSS:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
 - **Regla versión:** product_version: “19.2 <19.2.5” -> (Cumple condiciones: Rama/Coincidencia 19.2 (Sí) | 19.2.4 < 19.2.5 (Sí))
 - **Justificación / Descripción:** > GitLab has remediated an issue in GitLab EE affecting all versions from 11.10 before 19.1.7, 19.2 before 19.2.5, and 19.3 before 19.3.1 that, under certain conditions, an authentic...
-

[MEDIA] - EUVD-2026-70117 - GHSA-j4r9-h92x-jjh3

- **Producto / Versión:** Jenkins (v2.568.1) | **Fuente:** ENISA

- **BaseScore:** 6.3 3.1 | **Parcheo Vulnerabilidad:** Diferible
 - **Vector CVSS:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L
 - **Regla versión:** product_version: “patch: 2.568.3” -> (2.568.1 anterior al parche 2.568.3)
 - **Justificación / Descripción:** > In Jenkins 2.579 and earlier, LTS 2.568.2 and earlier, the REST API and CLI endpoints for updating agent configuration do not prevent a submitted configuration from overwriting a d...
-

[MEDIA] - EUVD-2026-66431 - GHSA-46vv-8gc3-7xrq

- **Producto / Versión:** GitLab CE (v19.2.4) | **Fuente:** ENISA
 - **BaseScore:** 5.5 3.1 | **Parcheo Vulnerabilidad:** Descartable
 - **Vector CVSS:** CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:N
 - **Regla versión:** product_version: “19.2 <19.2.5” -> (Cumple condiciones: Rama/Coincidencia 19.2 (Sí) | 19.2.4 < 19.2.5 (Sí))
 - **Justificación / Descripción:** > GitLab has remediated an issue in GitLab EE affecting all versions from 11.3 before 19.1.7, 19.2 before 19.2.5, and 19.3 before 19.3.1 that, under certain conditions, an authentica...
-

[MEDIA] - EUVD-2026-70120 - GHSA-jrvc-6cvv-qqx5

- **Producto / Versión:** Jenkins (v2.568.1) | **Fuente:** ENISA
 - **BaseScore:** 5.4 3.1 | **Parcheo Vulnerabilidad:** Diferible
 - **Vector CVSS:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N
 - **Regla versión:** product_version: “patch: 2.568.3” -> (2.568.1 anterior al parche 2.568.3)
 - **Justificación / Descripción:** > In Stapler 2107.v8dfcb_e8ed317 and earlier, except 2088.2093.vd7c3e58008a_6, included in Jenkins 2.579 and earlier, LTS 2.568.2 and earlier, form data binding allows setting public...
-

[MEDIA] - EUVD-2026-67167 - GHSA-hpxp-rx7c-457j

- **Producto / Versión:** GitLab CE (v19.2.4) | **Fuente:** ENISA
 - **BaseScore:** 5.4 3.1 | **Parcheo Vulnerabilidad:** Diferible
 - **Vector CVSS:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N
 - **Regla versión:** product_version: “19.2 <19.2.5” -> (Cumple condiciones: Rama/Coincidencia 19.2 (Sí) | 19.2.4 < 19.2.5 (Sí))
 - **Justificación / Descripción:** > GitLab has remediated an issue in GitLab EE affecting all versions from 18.3 before 19.1.7, 19.2 before 19.2.5, and 19.3 before 19.3.1 that, under certain conditions, an authentica...
-

[MEDIA] - EUVD-2026-70112 - CVE-2026-84646

- **Producto / Versión:** Jenkins (v2.568.1) | **Fuente:** ENISA
 - **BaseScore:** 4.3 3.1 | **Parcheo Vulnerabilidad:** Diferible
 - **Vector CVSS:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N
 - **Regla versión:** product_version: “patch: 2.580” -> (2.568.1 anterior al parche 2.580)
 - **Justificación / Descripción:** > In Jenkins 2.579 and earlier, LTS 2.568.2 and earlier, user objects can appear as nested field values in other deserialized XML objects, allowing attackers with Overall/Read permis...
-

[MEDIA] - EUVD-2026-70121 - CVE-2026-84655

- **Producto / Versión:** Jenkins (v2.568.1) | **Fuente:** ENISA
- **BaseScore:** 4.3 3.1 | **Parcheo Vulnerabilidad:** Diferible
- **Vector CVSS:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N
- **Regla versión:** product_version: “patch: 2.580” -> (2.568.1 anterior al parche 2.580)
- **Justificación / Descripción:** > Jenkins 2.579 and earlier, LTS 2.568.2 and earlier does not escape map keys when serializing objects as JSON and Python through its REST API, allowing attackers able to control map...

[MEDIA] - EUVD-2026-70122 - GHSA-9v33-56f7-qg5c

- **Producto / Versión:** Jenkins (v2.568.1) | **Fuente:** ENISA
- **BaseScore:** 4.3 3.1 | **Parcheo Vulnerabilidad:** Diferible
- **Vector CVSS:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N
- **Regla versión:** product_version: "patch: 2.568.3" -> (2.568.1 anterior al parche 2.568.3)
- **Justificación / Descripción:** > A missing permission check in Jenkins 2.579 and earlier, LTS 2.568.2 and earlier allows attackers with Item/Read permission on at least one job to read build parameter names and va...

[MEDIA] - EUVD-2026-53570 - CVE-2026-70427

- **Producto / Versión:** Jenkins (v2.568.1) | **Fuente:** ENISA
- **BaseScore:** 4.3 3.1 | **Parcheo Vulnerabilidad:** Diferible
- **Vector CVSS:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N
- **Regla versión:** product_version: "patch: 2.576" -> (2.568.1 anterior al parche 2.576)
- **Justificación / Descripción:** > Jenkins 2.575 and earlier, LTS 2.568.1 and earlier does not safely handle symbolic links with effectively empty names during the extraction of .tar and .tar.gz archives, allowi...

[MEDIA] - EUVD-2026-53571 - GHSA-c232-r242-w9v9

- **Producto / Versión:** Jenkins (v2.568.1) | **Fuente:** ENISA
- **BaseScore:** 4.3 3.1 | **Parcheo Vulnerabilidad:** Diferible
- **Vector CVSS:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N
- **Regla versión:** product_version: "patch: 2.576" -> (2.568.1 anterior al parche 2.576)
- **Justificación / Descripción:** > Jenkins 2.575 and earlier, LTS 2.568.1 and earlier improperly identifies file paths attempting path traversal in file parameter names, allowing attackers with Item/Configure and It...

[MEDIA] - EUVD-2026-66429 - GHSA-8x29-wc3v-56mg

- **Producto / Versión:** GitLab CE (v19.2.4) | **Fuente:** ENISA
- **BaseScore:** 4.3 3.1 | **Parcheo Vulnerabilidad:** Diferible
- **Vector CVSS:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N
- **Regla versión:** product_version: "19.2 <19.2.5" -> (Cumple condiciones: Rama/Coincidencia 19.2 (Sí) | 19.2.4 < 19.2.5 (Sí))
- **Justificación / Descripción:** > GitLab has remediated an issue in GitLab EE affecting all versions from 19.1 before 19.1.7, 19.2 before 19.2.5, and 19.3 before 19.3.1 that, under certain conditions, an authentica...

[MEDIA] - EUVD-2026-70123 - CVE-2026-84657

- **Producto / Versión:** Jenkins (v2.568.1) | **Fuente:** ENISA
- **BaseScore:** 4.2 3.1 | **Parcheo Vulnerabilidad:** Diferible
- **Vector CVSS:** CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:L
- **Regla versión:** product_version: "patch: 2.568.3" -> (2.568.1 anterior al parche 2.568.3)
- **Justificación / Descripción:** > In Jenkins 2.579 and earlier, LTS 2.568.2 and earlier, the build CLI command does not check the Item/Cancel permission when using the -s flag to cancel a build triggered to wait fo...

[BAJA] - EUVD-2026-66430 - GHSA-r8m7-3v38-qjrm

- **Producto / Versión:** GitLab CE (v19.2.4) | **Fuente:** ENISA
- **BaseScore:** 3.5 3.1 | **Parcheo Vulnerabilidad:** Diferible

- **Vector CVSS:** CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:N
 - **Regla versión:** product_version: “19.2 <19.2.5” -> (Cumple condiciones: Rama/Coincidencia 19.2 (Sí) | 19.2.4 < 19.2.5 (Sí))
 - **Justificación / Descripción:** > GitLab has remediated an issue in GitLab EE affecting all versions from 13.1 before 19.1.7, 19.2 before 19.2.5, and 19.3 before 19.3.1 that, under certain conditions, an authentica...
-

[BAJA] - EUVD-2026-53524 - CVE-2026-70430

- **Producto / Versión:** Jenkins (v2.568.1) | **Fuente:** ENISA
 - **BaseScore:** 2.7 3.1 | **Parcheo Vulnerabilidad:** Descartable
 - **Vector CVSS:** CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N
 - **Regla versión:** product_version: “patch: 2.568.2” -> (2.568.1 anterior al parche 2.568.2)
 - **Justificación / Descripción:** > Jenkins 2.575 and earlier, LTS 2.568.1 and earlier does not restrict the types of objects that can be instantiated as part of the project naming strategy configuration, allowing at...
-

[BAJA] - EUVD-2026-70118 - CVE-2026-84652

- **Producto / Versión:** Jenkins (v2.568.1) | **Fuente:** ENISA
 - **BaseScore:** 0.0 3.1 | **Parcheo Vulnerabilidad:** Diferible
 - **Vector CVSS:** N/A
 - **Regla versión:** product_version: “patch: 2.568.3” -> (2.568.1 anterior al parche 2.568.3)
 - **Justificación / Descripción:** > In Jenkins 2.579 and earlier, LTS 2.568.2 and earlier, Jenkins does not rotate the session when a user is authenticated via the “remember me” cookie, allowing attackers able to ser...
-

[BAJA] - EUVD-2026-70119 - CVE-2026-84653

- **Producto / Versión:** Jenkins (v2.568.1) | **Fuente:** ENISA
 - **BaseScore:** 0.0 3.1 | **Parcheo Vulnerabilidad:** Diferible
 - **Vector CVSS:** N/A
 - **Regla versión:** product_version: “patch: 2.580” -> (2.568.1 anterior al parche 2.580)
 - **Justificación / Descripción:** > Jenkins 2.421 through 2.579 (both inclusive), LTS 2.426.1 through 2.568.2 (both inclusive) does not correctly perform permission checks in the Appearance configuration page, allowi...
-