Informe técnico – Top 10 hallazgos críticos/alto (Prowler)

Generado: 2025-10-06 13:57:19Z (UTC)

Origen: archivo `scan-0199a01e-6cf5-71e3-b791-bfcf0e47e07f-report.zip` — `prowler-output-MoroLitZ-20251001141431.ocsf.json`

Índice

---

1. Resumen ejecutivo

- Se extrajeron 18 hallazgos con estado FAIL y severidad High/Critical.

- Este documento presenta los 10 hallazgos más importantes, su análisis de causa raíz y pasos técnicos concretos para subsanarlos.

---

2. Metodología

- Se procesó el archivo OCSF/JSON generado por Prowler dentro del ZIP.

- Se filtraron resultados con `status_code=FAIL` y `severity` en {High, Critical}.

- Se seleccionaron las primeras 10 entradas ordenadas por severidad y aparición para análisis manual y generación de remediaciones.

---

3. Hallazgos top 10 (detallados)

1. ID: `` — Recurso: `` — Severidad: **Critical**

- **Título / comprobación:**

- **Descripción:**

```

```

- **Mensaje bruto Prowler (extracto):** Repository ingecarplus-main does not enforce branch protection on default branch (main).

- **Análisis del porqué del fallo (causa raíz):**

Configuración insegura o ausencia de controles de protección en el repositorio/pipeline relacionado.

- **Remediación sugerida (resumen):**

- Review the detailed Prowler finding and the resource configuration in the repository settings or organization policy.

- Apply principle of least privilege and enforce branch protection rules.

- Document and automate checks in CI to prevent recurrence.

- Nota: Check vendor docs and CIS/GitHub security guidance.

---

2. ID: `` — Recurso: `` — Severidad: **Critical**

- **Título / comprobación:**

- **Descripción:**

```

```

- **Mensaje bruto Prowler (extracto):** Repository Manim does not enforce branch protection on default branch (main).

- **Análisis del porqué del fallo (causa raíz):**

Configuración insegura o ausencia de controles de protección en el repositorio/pipeline relacionado.

- **Remediación sugerida (resumen):**

- Review the detailed Prowler finding and the resource configuration in the repository settings or organization policy.

- Apply principle of least privilege and enforce branch protection rules.

- Document and automate checks in CI to prevent recurrence.

- Nota: Check vendor docs and CIS/GitHub security guidance.

---

3. ID: `` — Recurso: `` — Severidad: **High**

- **Título / comprobación:**

- **Descripción:**

```

```

- **Mensaje bruto Prowler (extracto):** Repository ingecarplus-main does allow default branch deletion.

- **Análisis del porqué del fallo (causa raíz):**

Configuración insegura o ausencia de controles de protección en el repositorio/pipeline relacionado.

- **Remediación sugerida (resumen):**

- Review the detailed Prowler finding and the resource configuration in the repository settings or organization policy.

- Apply principle of least privilege and enforce branch protection rules.

- Document and automate checks in CI to prevent recurrence.

- Nota: Check vendor docs and CIS/GitHub security guidance.

---

4. ID: `` — Recurso: `` — Severidad: **High**

- **Título / comprobación:**

- **Descripción:**

```
```

```

- **Mensaje bruto Prowler (extracto):** Repository Manim does allow default branch deletion.

- **Análisis del porqué del fallo (causa raíz):**

Configuración insegura o ausencia de controles de protección en el repositorio/pipeline relacionado.

- **Remediación sugerida (resumen):**

- Review the detailed Prowler finding and the resource configuration in the repository settings or organization policy.

- Apply principle of least privilege and enforce branch protection rules.

- Document and automate checks in CI to prevent recurrence.

- Nota: Check vendor docs and CIS/GitHub security guidance.

---

### 5. ID: `` — Recurso: `` — Severidad: **High**

- **Título / comprobación:**

- **Descripción:**

```

```

- **Mensaje bruto Prowler (extracto):** Repository ingecarplus-main does allow force pushes on default branch (main).

- **Análisis del porqué del fallo (causa raíz):**

Configuración insegura o ausencia de controles de protección en el repositorio/pipeline relacionado.

- **Remediación sugerida (resumen):**

- Review the detailed Prowler finding and the resource configuration in the repository settings or organization policy.

- Apply principle of least privilege and enforce branch protection rules.

- Document and automate checks in CI to prevent recurrence.

- Nota: Check vendor docs and CIS/GitHub security guidance.
```

---

6. ID: `` — Recurso: `` — Severidad: **High**

- **Título / comprobación:**

- **Descripción:**

```

```

- **Mensaje bruto Prowler (extracto):** Repository Manim does allow force pushes on default branch (main).

- **Análisis del porqué del fallo (causa raíz):**

Configuración insegura o ausencia de controles de protección en el repositorio/pipeline relacionado.

- **Remediación sugerida (resumen):**

- Review the detailed Prowler finding and the resource configuration in the repository settings or organization policy.

- Apply principle of least privilege and enforce branch protection rules.

- Document and automate checks in CI to prevent recurrence.

- Nota: Check vendor docs and CIS/GitHub security guidance.

---

7. ID: `` — Recurso: `` — Severidad: **High**

- **Título / comprobación:**

- **Descripción:**

```

```

- **Mensaje bruto Prowler (extracto):** Repository ingecarplus-main does not enforce administrators to be subject to the same branch protection rules as other users.

- **Análisis del porqué del fallo (causa raíz):**

Configuración insegura o ausencia de controles de protección en el repositorio/pipeline relacionado.

- **Remediación sugerida (resumen):**

- Review the detailed Prowler finding and the resource configuration in the repository settings or organization policy.

- Apply principle of least privilege and enforce branch protection rules.

- Document and automate checks in CI to prevent recurrence.

- Nota: Check vendor docs and CIS/GitHub security guidance.

---

8. ID: `` — Recurso: `` — Severidad: **High**

- **Título / comprobación:**

- **Descripción:**

```

```

- **Mensaje bruto Prowler (extracto):** Repository Manim does not enforce administrators to be subject to the same branch protection rules as other users.

- **Análisis del porqué del fallo (causa raíz):**

Configuración insegura o ausencia de controles de protección en el repositorio/pipeline relacionado.

- **Remediación sugerida (resumen):**

- Review the detailed Prowler finding and the resource configuration in the repository settings or organization policy.

- Apply principle of least privilege and enforce branch protection rules.

- Document and automate checks in CI to prevent recurrence.

- Nota: Check vendor docs and CIS/GitHub security guidance.

---

9. ID: `` — Recurso: `` — Severidad: **High**

- **Título / comprobación:**

- **Descripción:**

```
```

```

- **Mensaje bruto Prowler (extracto):** Repository ingecarplus-main does not require code owner approval for changes to owned code.

- **Análisis del porqué del fallo (causa raíz):**

Configuración insegura o ausencia de controles de protección en el repositorio/pipeline relacionado.

- **Remediación sugerida (resumen):**

- Review the detailed Prowler finding and the resource configuration in the repository settings or organization policy.

- Apply principle of least privilege and enforce branch protection rules.

- Document and automate checks in CI to prevent recurrence.

- Nota: Check vendor docs and CIS/GitHub security guidance.

---

### 10. ID: `` — Recurso: `` — Severidad: **High**

- **Título / comprobación:**

- **Descripción:**

```

```

- **Mensaje bruto Prowler (extracto):** Repository Manim does not require code owner approval for changes to owned code.

- **Análisis del porqué del fallo (causa raíz):**

Configuración insegura o ausencia de controles de protección en el repositorio/pipeline relacionado.

- **Remediación sugerida (resumen):**

- Review the detailed Prowler finding and the resource configuration in the repository settings or organization policy.

- Apply principle of least privilege and enforce branch protection rules.

- Document and automate checks in CI to prevent recurrence.
```

- Nota: Check vendor docs and CIS/GitHub security guidance.

---

4. Remediaciones técnicas paso a paso (con comandos y UI)

A. Proteger la rama por defecto (UI)

1. Accede al repositorio en GitHub → Settings → Branches → Branch protection rules.

2. Click 'Add rule' y en 'Branch name pattern' escribe `main` o el nombre de la rama por defecto.

3. Marca opciones recomendadas:

- 'Require pull request reviews before merging' (configura al menos 1-2 revisores).

- 'Require status checks to pass before merging' y selecciona checks relevantes.

- 'Require branches to be up to date before merging' (opcional pero recomendado).

- 'Restrict who can push to matching branches' (define equipos o personas con push permitido).

- 'Do not allow deletion of the branch' (impedir la eliminación del branch protegido).

4. Save changes.

Referencias: https://docs.github.com/en/repositories/configuring-branches-and-merges-in-your-repository/managing-protected-branches/managing-a-branch-protection-rule

B. Remediar secrets expuestos (comandos y pasos)

1. Rotar secrets / revocar tokens inmediatamente.

2. Limpiar historial git (ejemplo con `git filter-repo`):

```bash
pip install git-filter-repo
# clona el repo
git clone --mirror https://github.com/ORG/REPO.git
cd REPO.git
# eliminar archivo que contiene secret
git filter-repo --path filename_with_secret --invert-paths
```

push force al repo remoto (coordinado con el equipo)

git push --force --all

```

3. Habilitar secret scanning y push protection en GitHub Enterprise / GitHub Advanced Security.

### C. Ajustes en GitHub Actions

- Definir `permissions` en workflows para el mínimo necesario, ejemplo:

```yaml

permissions:

contents: read

id-token: write

actions: read

```

- Evitar exponer secrets a forks: usar `pull_request_target` con cuidado y preferir `pull_request` with limited permissions.

- Pin actions to specific commit SHAs to avoid supply-chain risks.

---

5. Prioridad y roadmap de implementación

- **Fase 0 (24h):** Revocar tokens/secrets encontrados; desactivar ability to delete default branches; aislar repositorios críticos.

- **Fase 1 (1 semana):** Implementar branch protection rules en repos críticos; habilitar status checks y secret scanning.

- **Fase 2 (1 mes):** Revisar workflows y permisos; integrar análisis SCA/Dependabot; formar equipo de respuesta.

- **Fase 3 (3 meses+):** Automatizar remediaciones y consolidar en SIEM/GRC.

---

6. Anexos y evidencias

- Archivo JSON original dentro del ZIP: `prowler-output-MoroLitZ-20251001141431.ocsf.json` (contiene todos los hallazgos).
```

- Se recomienda revisar las entradas completas allí para cada 'id' presentado.