



SAMPLE

Restricted Collaborator Role Exposes Metadata of Unshared Related Observations

SecurityTrackr

RISK RATING

VERY LOW

STATUS

● Mitigated

LIKELIHOOD

Highly unlikely

IMPACT

Low

REGISTERED

22 September 2026

AUTHOR

REDACTED

OBSERVATION SUMMARY

WHAT WE FOUND

SecurityTrackr's "restricted collaborator" role gives an invited user no read access to the security register; a separate "Shared with me" screen lists only observations a member or owner explicitly shared. The typical case is a single-system specialist, say an Exchange admin, needing one observation. The original design also surfaced metadata for related observations linked to those shared: title, risk scoring, framework alignment, and the AI-generated comment justifying the link, once a collaborator or above had accepted the relationship. An internal AI-based penetration test flagged it as a design flaw; the metadata was stripped from that view entirely in September 2026 and re-tested against a specific access control matrix with real adversarial calls.

WHY IT MATTERS

The role's whole point is least privilege, and the old behaviour broke that promise: a restricted collaborator learned the existence, title, risk rating and framework context of observations nobody chose to share. Titles and AI relationship justifications are descriptive, so the metadata alone could reveal weaknesses in systems outside the user's remit, useful reconnaissance for an external or contractor account scoped to one system. With the metadata gone the role now matches what customers were sold, and sharing is explicit: members must share every observation a restricted collaborator needs directly, rather than relying on a per-relationship opt-in.

LIKELIHOOD

The disclosure path is gone. Related-observation metadata no longer renders in the "Shared with me" view at all, and the fix was verified after the fact against an access control matrix using real adversarial calls, not just a code read. A restricted collaborator now sees only what a member or owner hands them directly, so harm would need a regression to reintroduce the old behaviour.



IMPACT

Even before the fix, what leaked was metadata: titles, risk scores, framework alignment and the AI justification for a link. No observation bodies, evidence or credentials were exposed, and nothing crossed a tenant boundary. Today nothing surfaces beyond the observations deliberately shared, so any consequence from a regression stays bounded to in-tenant weakness metadata for a single organisation.

RESIDUAL RISK

What's left is regression: a future change to the sharing or relationship code could put related-observation metadata back in the "Shared with me" view, re-exposing weakness titles and risk scores to an invited, often external, user. The structural controls still cap it: no register-wide read access, sharing stays owner or member driven, and testing found no cross-tenant IDOR or other authorisation flaws in the role.

AFFECTED SYSTEMS

SecurityTrackr multi-tenant SaaS application (security observation register), restricted collaborator role, "Shared with me" view, related-observations metadata

MITIGATING CONTROLS

- The restricted collaborator role grants no read access to the main security register; the user only gets a separate "Shared with me" view.
- That view lists only observations explicitly shared by a member or owner.
- Related-observation metadata is only surfaced once the relationship has been identified and accepted by a user holding collaborator role or above.
- Exposure is bounded to a single organisation: penetration testing found no tenant-level IDOR issues.
- Penetration testing found no other authorisation flaws in the restricted collaborator role.

RECOMMENDATIONS

- ✓ Remove related-observation metadata (title, risk score, framework alignment, AI justification) from the restricted collaborator's 'Shared with me' view entirely; only show the specific observations that were explicitly shared. (Completed)
Risk reduction Near-total Ease of implementation Moderate effort
- ✗ Make the surfacing of related-observation metadata an explicit per-relationship opt-in that the sharing member or owner must switch on, defaulting to off for restricted collaborators. (Won't Do)
Risk reduction Substantial Ease of implementation Moderate effort
- ✗ If some visibility into related observations must stay, redact the risk score and AI-generated justification and replace the descriptive title with a generic 'related item exists' flag. (Won't Do)
Risk reduction Moderate Ease of implementation Straightforward

ISO 27002:2022 AREAS

5.15 — Access control (primary)

8.3 — Information access restriction

5.18 — Access rights



NIST CSF 2.0 AREAS

Protect

Identify