COMMUNITY CONTENT

Home › Submit › 780607

Submit #780607: z-9527 admin ≤ commit 72aaf2d Dynamically-Determined Object Attributes

Title	z-9527 admin ≤ commit 72aaf2d Dynamically-Determined Object Attributes
Description	A mass assignment vulnerability exists in Z-9527 Admin ≤ commit 72aaf2d at the /user/update endpoint, where user-supplied parameters are directly iterated and incorporated into SQL UPDATE statements without field whitelisting. As a result, authenticated attackers can modify arbitrary database columns, including privilege-escalation fields such as isAdmin. Mitigations include implementing a strict whitelist of updatable fields, using an ORM with explicit field mapping, validating all input parameters against allowed attributes, separating privileged fields into admin-only update routes, and applying role-based access control before processing any update operations.
Source	⚠ https://github.com/CC-T-454455/Vulnerabilities/tree/master/z9527-admin/vulnerability-11
User	Anonymous User
Submission	03/16/2026 04:37 AM (16 days ago)
Moderation	03/31/2026 06:11 PM (16 days later)
Status	Accepted
VulDB entry	354441 [z-9527 admin 1.0/2.0 User Update Endpoint /server/routes/user.js isAdmin dynamically-determined object attributes]
Points	20

Community Content

Submissions are made by VulDB community users. VulDB is *not responsible* for their content nor the links to external sources.

Please use the raw information shown and the links listed *with caution*. They might contain malicious and harmful actions, code or data.

The corresponding VulDB entries contain the moderated, verified, and normalized information provided within the raw submission.

Documentation

- Submission Policy
- Data Processing
- CVE Handling