VULNERABILITY RESEARCH

CVE-2026-79957 Insecure Direct Objec Reference in ServiceNext

MARK GADDY
OCT 14, 2026



Overview

ServiceNext contains an insecure direct object reference (IDOR) CVE-2026-79957 i the /api/Usuario/GetUsuarios endpoint, which accepts a user-controlled numeric ID the request body without verifying that the authenticated token belongs to the

requested account (CWE-639). Any authenticated user can iterate the ID parameter retrieve the full profile record of every other user, including passwords stored in cleartext (CWE-256), enabling account takeover and credential-stuffing attacks.

The Vulnerability

ServiceNext exposes a user information retrieval endpoint, POST /api/Usuario/GetUsuarios, that accepts a numeric user identifier (ID) in the body of request. The endpoint confirms that the caller presents a valid authentication toker but it never confirms that the token actually belongs to the account named in the II field.

Changing the ID value to a number that does not belong to the caller returns the fu profile for that other user. No error, no authorization failure, just another user's record. The identifiers are sequential integers, so walking the ID value from one number to the next enumerates the entire user population, and a single authenticat user can retrieve every account in the application in one automated pass.

Why It Matters

Each record includes the username, display name, assigned partner company, recov email, and the account password, which ServiceNext stores and returns in cleartext No cracking is required: one valid account pulls working credentials for every user, and reused passwords lead directly to account takeover and credential-stuffing agai other services. The exposed partner associations are a secondary disclosure of sensitive business data.

Proof of Concept

Authenticate with any valid account, capture the bearer token, and send a GetUsua request with an ID belonging to a different user. Identifying values are replaced wit placeholders:

```
curl -sk -X POST “https://<redacted>.servicenext.eu/api/Usuario/GetUsuarios” \
-H “Content-Type: application/json” \
-H “Origin: https://<redacted>.servicenext.eu” \
-H “Referer: https://<redacted>.servicenext.eu/” \
-d ‘{”REGSPAGE”:1,”PAGE”:1,”ORDERCOLUM”:1,”ORDERDIR”:”A”,”ID”:<target_id>,
“ID_TALLER”:0,”BAJA”:0,”RAZON_SOCIO”:””,”NOMBRE_TALLER”:””,
“Token”:”<auth_token>”}’
```

The response contains the target user’s full record, including the cleartext passwor regardless of which token was presented:

```
{
  “OK”: true,
    “USUARIOS”: [{
      “ID”: <target_id>,
      “USUARIO”: “<username>”,
      “PWD”: “<cleartext_password>”,
      “NOMBRE_USUARIO”: “<display_name>”,
      “ID_SOCIO”: <partner_id>,
      “RAZON_SOCIO”: “<partner_company_name>”,
      “CORREO_RECUPERACION_PWD”: “<recovery_email>”
    }]
}
```

Iterating the ID value across the valid range enumerates every account in the application.

Remediation

ServiceNext has fully remediated this vulnerability in a subsequent release. Update the latest version of ServiceNext, which adds the missing server-side authorization check.

Disclosure Timeline

2026/06/24: Vulnerability discovered and verified during a customer assessment.

2026/06/25: Responsible disclosure process initiated and technical details documen

2026/08/24: ServiceNext acknowledged the report and released a version that fully remediates the vulnerability.

2026/10/14: Public disclosure.

Subscribe to Black Lantern Security (BLSOPS)

Launched 5 years ago

Timely research, discussion, and tactics for Cybersecurity leadership, operators, and analys

Type your email... Subscribe

By subscribing, you agree to Substack's Terms of Use, and acknowledge its Information Collection Notice and Privacy Policy.

Discussion about this post

Comments Restacks

Write a comment...

© 2026 Black Lantern Security (BLSOPS) · Privacy • Terms • Collection notice
Substack is the home for great culture