elmec

CVE-2026-51367: Insecure Direct Object Reference (IDOR) Leading to Unauthorized Data Access



Scritto da **Andrea Ferrario**

Summary

Field	Value
CVE ID	CVE-2026-51367
Product	Vedo Suite (Bottinelli Informatica)
Affected Version(s)	v1.2.5
Vulnerability Class	CWE-639: Authorization Bypass Through User-Controlled Key
Attack Vector	Network (HTTP API)
Privileges Required	Low (authenticated application user)
User Interaction	None
Impact	Confidentiality breach / unauthorized access to other users' data
Estimated CVSS 3.1	8.7 (High) — AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/
Estimated CVSS 3.1	9.9 (Critical) — AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H /A:H

Affected Components

The vulnerability affects multiple API endpoints where user-controlled identifiers are used to retrieve private user-specific resources without enforcing proper server-

side authorization checks.

Affected endpoints:

- POST /api_vedo/dati-ftp?utente_ftp=username
- GET /api_vedo/chat?utente_chat=username

The parameters utente_ftp and utente_chat are accepted from the client and used to reference user-specific resources. However, the application does not properly verify that the authenticated user is authorized to access the requested object.

Vulnerability Description

An authenticated low-privileged user can modify the utente_ftp or utente_chat parameter to reference another valid user identifier. Due to missing object-level authorization controls, the application returns information belonging to other users.

This is a classic case of **Insecure Direct Object Reference (IDOR)**, where internal object identifiers are exposed through user-controlled parameters and access control is not enforced server-side.

Exploitation Characteristics

Exploitation requires:

- A valid authenticated account with low privileges.
- Knowledge or enumeration of another valid username identifier.
- Modification of the affected parameter within an HTTP request.

No user interaction is required.

Example exploitation scenarios:

- POST /api_vedo/dati-ftp?utente_ftp=

Cerca nel blog

attacker may retrieve resources associated with that account.

Impact

Ultimi post pubblicati

Successful exploitation allows an authenticated attacker to:

Ivana Basaric 8/24/2026

Paolo Ferro 7/31/2026

Andrea Ferrario 7/30/2026

Andrea Ferrario 7/30/2026

- Access private chat communications belonging to other users.
- Retrieve unauthorized FTP-related user information.
- Violate confidentiality of user-specific application data.

The vulnerability has a high confidentiality impact because private communications and user-specific resources can be accessed without authorization.

CWE Mapping

- **CWE-639** — Authorization Bypass Through User-Controlled Key
- **CWE-284** — Improper Access Control
- **OWASP API Security Top 10: API1: Broken Object Level Authorization (BOLA)**

Root Cause

The root cause is the absence of server-side authorization checks before returning user-specific

50annidiElmec About AI as400
ASSET MANAGEMENT automation award
backup business continuity career cloud
CMDB competenze comunicato connect
connettività container CSR cybersecurity
data center data management
data protection data security
device as a service devops dex
digital employee esperience
digital infrastructure digital workplace
disaster recovery elmec Elmec Vision
events formazione governance help desk
HR hybrid cloud ibm Infrastructure IT
IoT IT operation macchine virtuali
managed Licensing Service Managed Workplace
myelmec network news noleggio
noleggio operativo patch patch management
Platform Services postazioni di lavoro
press release SAP sase sdwan
security servizi gestiti sistemi informatici
Sostenibilità Sponsored Blog Post Storage
ticketing virtual machine vpn workplace
ztna

Mitigation and Remediation

Evidence Handling

Screenshots demonstrating unauthorized access are intentionally omitted from this advisory because the affected information contains restricted user data and private communications.

The vulnerability was validated through controlled testing by modifying the affected parameters and confirming unauthorized access behavior.

References

- **CWE-639 — Authorization Bypass Through User-Controlled Key**
  https://cwe.mitre.org/data/definitions/639.html
  :contentReferenceoaicite:1
- **CWE-284 — Improper Access Control**
  https://cwe.mitre.org/data/definitions/284.html
  :contentReferenceoaicite:2
- **OWASP API Security Top 10 — API1: Broken Object Level Authorization (BOLA)**
  - API1:2023 — Broken Object Level Authorization
    https://owasp.org/API-Security/editions/2023/en/0xa1-broken-object-level-authorization/
  - API1:2019 — Broken Object Level Authorization
    https://owasp.org/API-Security/editions/2019/en/0xa1-broken-object-level-authorization/
    :contentReferenceoaicite:3

Credits

Andrea Ferrario, Stefano Andreatta, CybergON

elmec
LinkedIn Instagram Facebook
+39 0332.802.111
Note legali
Assistenza tecnica
CHI SIAMO
Non possiamo parlare di futuro senza raccontarti le origini. Era il 1971 quando tutto ebbe inizio. Una storia lunga quanto quella dell'informatica: c'era la perforatrice e c'eravamo noi.
Guarda come siamo diventati grandi.

Lavora con noi

Privacy Policy | Cookies Policy | Informativa privacy clienti e fornitori Elmec Informatica S.p.A. © 2024 - Tutti i diritti sono riservati