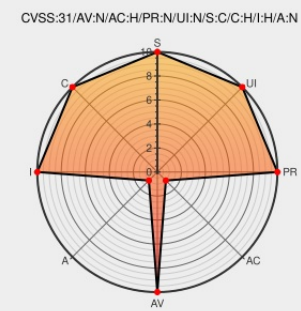
CVE-2021-45036

Published on: Not Yet Published

Last Modified on: 07/21/2023 04:45:00 PM UTC

CVE-2021-45036 - advisory for INCIBE-2022-1017

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Vclient from Velneo contain the following vulnerability:

Velneo vClient on its 28.1.3 version, could allow an attacker with knowledge of the victims's username and hashed password to spoof the victim's id against the server.

CVE-2021-45036 has been assigned by cve-coordination@incibe.es to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Velneo** - **Velneo vClient** version **= 28.1.3**

CVSS3 Score: 7.4 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	NONE

CVE References

Description	Tags	Link
Notas de la versión - Documentación de Velneo	doc.velneo.com application/octet-stream	MISC doc.velneo.com/v/32/velneo/notas-de-la-version#mejoras-de-seguridad-en-validacion-de-usuario-y-contrasena
Nueva versión Velneo 32	www.velneo.com text/html	MISC www.velneo.com/blog/disponible-la-nueva-version-velneo-32
Conexión con Velneo vServer - Documentación de Velneo	doc.velneo.com application/octet-stream	MISC doc.velneo.com/v/32/velneo/funcionalidades-comunes/conexion-con-velneo-vserver
Protocolo VATPS - Documentación de Velneo	doc.velneo.com application/octet-stream	MISC doc.velneo.com/v/32/velneo-vserver/funcionalidades/protocolo-vatps
Listado de cambios Velneo 32.0 | Velneo	velneo.es text/html	MISC velneo.es/mivelneo/listado-de-cambios-velneo-32/

Notas de la versión - Documentación de Velneo	doc.velneo.com application/octet-stream	MISC doc.velneo.com/v/32/velneo/notas-de-la-version#a-partir-de-esta-version-todos-los-servidores-arrancaran-con-protocolo-vatps
Velneo vClient improper authentication | INCIBE-CERT	www.incibe-cert.es text/html	CONFIRM www.incibe-cert.es/en/early-warning/security-advisories/velneo-vclient-improper-authentication-0

There are currently no QIDs associated with this CVE

Exploit/POC from Github

This repository contains a collection of data files on known Common Vulnerabilities and Exposures (CVEs). Each file i…

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Velneo	Vclient	28.1.3	All	All	All

cpe:2.3:a:velneo:vclient:28.1.3:*:*:*:*:*:*:*:

Discovery Credit

Jesús Ródenas Huerta, @Marmeus

Social Mentions

Source	Title	Posted (UTC)
@incibe_cert	⚠ Autenticación incorrecta en #Velneo vClient. #0day #CNA #CVE CVE-2021-45036 incibe-cert.es/alerta-tempran…	2022-11-23 12:20:12
@CVEreport	CVE-2021-45036 : Velneo vClient on its 28.1.3 version, could allow an attacker with knowledge of the victims's user… twitter.com/i/web/status/1…	2022-11-28 16:07:43
/r/netcve	CVE-2021-45036	2022-11-28 17:38:28

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report