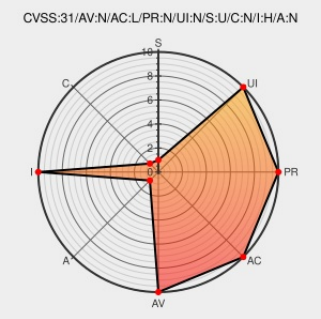
CVE-2021-4031

Published on: Not Yet Published

Last Modified on: 03/29/2022 02:44:00 PM UTC

CVE-2021-4031

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



Certain versions of Syltek from Syltek contain the following vulnerability:

Syltek application before its 10.22.00 version, does not correctly check that a product ID has a valid payment associated to it. This could allow an attacker to forge a request and bypass the payment system by marking items as payed without any verification.

CVE-2021-4031 has been assigned by cve-coordination@incibe.es to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Syltek** - **Syltek** version **< 10.22.00**

Vulnerability Patch/Work Around

This vulnerability has been solved by Playtomic in the in the 10.22.00 version.

CVSS3 Score: 7.5 - HIGH

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

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Syltek Insufficient Verification of Data Authenticity | INCIBE-CERT	www.incibe-cert.es text/html	CONFIRM www.incibe-cert.es/en/early-warning/security-advisories/syltek-insufficient-verification-data-authenticity

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Syltek	Syltek	All	All	All	All

cpe:2.3:a:syltek:syltek:*:*:*:*:*:*:*:*:

Discovery Credit

Enrique Benvenutto Navarro

Social Mentions

Source	Title	Posted (UTC)
@incibe_cert	⚠ Verificación insuficiente de la autenticidad de los datos en #Syltek #CNA #0day #CVE CVE-2021-4031 incibe-cert.es/alerta-tempran…	2022-03-14 07:38:33
@CVEreport	CVE-2021-4031 : Syltek application before its 10.22.00 version, does not correctly check that a product ID has a va… twitter.com/i/web/status/1…	2022-03-18 18:43:49
/r/netcve	CVE-2021-4031	2022-03-18 19:39:02

← Previous ID

Next ID→