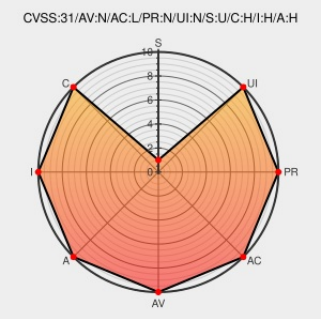
CVE-2022-32965

Published on: Not Yet Published

Last Modified on: 10/26/2022 02:49:00 AM UTC

CVE-2022-32965 - advisory for TVN-202206011

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



Certain versions of Omicard Edm from Omicard Edm Project contain the following vulnerability:

OMICARD EDM has a hard-coded machine key. An unauthenticated remote attacker can use the machine key to send serialized payload to the server to execute arbitrary code, manipulate system data and disrupt service.

CVE-2022-32965 has been assigned by cve@cert.org.tw to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **ITPison** - **OMICARD EDM** version **<= 6.0**

CVSS3 Score: 9.8 - CRITICAL

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

CVE References

Description	Tags	Link
CHT Security Red Team Discovered Vulnerability in Well-Known EDM System | 中華資安國際 CHT Security Co., Ltd.	www.chtsecurity.com text/html	MISC www.chtsecurity.com/news/48032532-b2de-401c-97a8-a2be5691988f
TWCERT/CC台灣電腦網路危機處理暨協調中心|企業資安通報協處|資安情資分享|漏洞通報|資安聯盟|資安電子報-沛盛資訊 OMICARD EDM行銷發送系統 - Use of Hard-coded Credentials	www.twcert.org.tw text/html	MISC www.twcert.org.tw/tw/cp-132-6373-34d51-1.html

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	Omicard Edm Project	Omicard Edm	All	All	All	All

cpe:2.3:a:omicard_edm_project:omicard_edm:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-32965 : OMICARD EDM has a hard-coded machine key. An unauthenticated remote attacker can use the machine k… twitter.com/i/web/status/1…	2022-08-04 09:20:06
@Robo_Alerts	Potentially Critical CVE Detected! CVE-2022-32965 OMICARD EDM has a hard-coded machine key. An unauthenticated remo… twitter.com/i/web/status/1…	2022-08-04 11:55:55
@threatmeter	CVE-2022-32965 OMICARD EDM has a hard-coded machine key. An unauthenticated remote attacker can use the machine key… twitter.com/i/web/status/1…	2022-08-05 07:09:43
@ColorTokensInc	Emerging Vulnerability Found CVE-2022-32965 - OMICARD EDM has a hard-coded machine key. An unauthenticated remote a… twitter.com/i/web/status/1…	2022-08-10 17:42:14
/r/netcve	CVE-2022-32965	2022-08-04 09:38:53

← Previous ID

Next ID→

© CVE.report 2023 | |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

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