



CVE-2023-22855

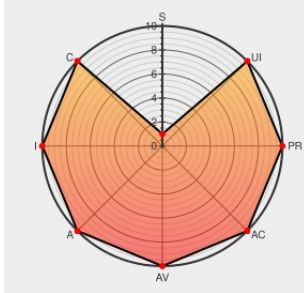
Published on: Not Yet Published

Last Modified on: 04/10/2023 09:15:00 PM UTC

CVE-2023-22855

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Kardex Control Center](#) from [Kardex](#) contain the following vulnerability:

Kardex Mlog MCC 5.7.12+0-a203c2a213-master allows remote code execution. It spawns a web interface listening on port 8088. A user-controllable path is handed to a path-concatenation method (Path.Combine from .NET) without proper sanitisation. This yields the possibility of including local files, as well as remote files on SMB

shares. If one provides a file with the extension .t4, it is rendered with the .NET templating engine mono/t4, which can execute code.

CVE-2023-22855 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

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
Kardex Mlog MCC 5.7.12+0-a203c2a213-master File Inclusion / Remote Code Execution ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/171046/Kardex-Mlog-MCC-5.7.12-0-a203c2a213-master-File-Inclusion-Remote-Code-Execution.html
CVE-2023-22855/advisory.md at main · patrickhener/CVE-2023-22855 · GitHub	github.com text/html	MISC github.com/patrickhener/CVE-2023-22855/blob/main/advisory/advisory.md
Kardex Mlog MCC 5.7.12 - RCE (Remote Code Execution) - Windows remote Exploit	www.exploit-db.com Proof of Concept text/html	MISC www.exploit-db.com/exploits/51239
Full Disclosure: Remote Code Execution in Kardex	seclists.org	FULLDISC 20230216 Remote Code Execution in

MLOG

text/html

Kardex MLOG

Kardex Mlog MCC 5.7.12 Remote Code Execution ≈ Packet Storm

packetstormsecurity.comtext/html

MISC packetstormsecurity.com/files/171689/Kardex-Mlog-MCC-5.7.12-Remote-Code-Execution.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

Exploit/POC from Github

Kardex Mlog MCC 5.7.12+0-a203c2a213-master allows remote code execution. It spawns a web interface listening on port ...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Kardex	Kardex Control Center	5.7.12\+0-a203c2a213-master	All	All	All

cpe:2.3:a:kardex:kardex_control_center:5.7.12\+0-a203c2a213-master:****:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@hack_git	CVE-2023-22855 This vulnerability was discovered and disclosed by Nico Viakowski and myself. This repository will... twitter.com/i/web/status/1...	2023-02-07 09:12:07
@ksg93rd	#exploit 1. CVE-2022-44268: ImageMagick arbitrary file read github.com/Vulnmachines/i... 2. CVE-2023-22855: Kardex Cont... twitter.com/i/web/status/1...	2023-02-07 12:35:06
@C1sc01	hsec.de/posts/cve-2023... Check out my writeup on my newest finding.	2023-02-07 15:00:43
@ThinkingObjects	Advisory: Kardex Mlog – Unsicherer Pfad in Verbindung mit SSTI führt zu RCE (CVE-2023-22855)... twitter.com/i/web/status/1...	2023-02-07 15:49:46
@CVEreport	CVE-2023-22855 : Kardex Mlog MCC 5.7.12+0-a203c2a213-master allows remote code execution. It spawns a web interface... twitter.com/i/web/status/1...	2023-02-15 21:06:58
/r/netcve	CVE-2023-22855	2023-02-15 22:38:28
/r/Team_IT_Security	#0daytoday #Kardex Mlog MCC 5.7.12 - Remote Code Execution Exploit CVE-2023-22855 [remote #exploits #0day #Exploit]	2023-04-05 21:29:24

← Previous ID

Next ID→

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 registered 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](#)