



CVE-2020-21503

Published on: 10/05/2021 12:00:00 AM UTC

Last Modified on: 10/14/2021 12:38:00 PM UTC

CVE-2020-21503

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

Certain versions of [Waimai Super Cms](#) from [Waimai Super Cms Project](#) contain the following vulnerability:

waimai Super Cms 20150505 has a logic flaw allowing attackers to modify a price, before form submission, by observing data in a packet capture. By setting the `index.php?m=gift&a=addsave credit` parameter to `-1`, the product is sold for free.

CVE-2020-21503 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

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
This is a payment logic vulnerability that can modify the value of payment · Issue #15 · caokang/waimai · GitHub	github.com text/html	MISC github.com/caokang/waimai/issues/15

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	Waimai Super Cms Project	Waimai Super Cms	20150505	All	All	All
cpe:2.3:a:waimai_super_cms_project:waimai_super_cms:20150505.*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2020-21503 : waimai Super Cms 20150505 has a logic flaw allowing attackers to modify a price, before form submi... twitter.com/i/web/status/1...	2021-10-05 22:05:23
 @WesUncensored	New vulnerability on the NVD: CVE-2020-21503 ift.tt/3FoeuT6	2021-10-06 00:33:09
 @workentin	New vulnerability on the NVD: CVE-2020-21503 ift.tt/3FoeuT6	2021-10-06 00:40:44
 @xanadulinux	CVE-2020-21503 ift.tt/3FoeuT6	2021-10-06 00:52:37
 @4ng3n01r3	#CyberSecurity #Security #CERT #CVE #Nist #breach #vulnerability : CVE-2020-21503	2021-10-10 06:55:04
 @4ng3n01r3	#CyberSecurity #Security #CERT #CVE #Nist #Analysed #breach #vulnerability : CVE-2020-21503 (waimai_super_cms)	2021-10-14 16:07:02

[← 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 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](#)