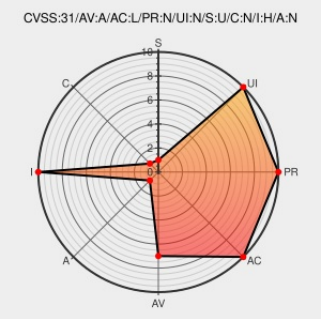
CVE-2023-34761

Published on: Not Yet Published

Last Modified on: 07/06/2023 04:10:00 PM UTC

CVE-2023-34761

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



Certain versions of Hello Cup from 7-eleven contain the following vulnerability:

An unauthenticated attacker within BLE proximity can remotely connect to a 7-Eleven LED Message Cup, Hello Cup 1.3.1 for Android, and bypass the application's client-side chat censor filter.

CVE-2023-34761 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.5 - MEDIUM

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

CVE References

Description	Tags	Link
GitHub - actuator/7-Eleven-Bluetooth-Smart-Cup-Jailbreak: 'Hacking' a 7-Eleven Bluetooth Smart Cup	github.com text/html	MISC github.com/actuator/7-Eleven-Bluetooth-Smart-Cup-Jailbreak
cve/CVE-2023-34761 at main · actuator/cve · GitHub	github.com text/html	MISC github.com/actuator/cve/blob/main/CVE-2023-34761

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	7-eleven	Hello Cup	1.3.1	All	All	All
Hardware	7-eleven	Led Message Cup	-	All	All	All

cpe:2.3:a:7-eleven:hello_cup:1.3.1:*:*:*:*:android:*:*:

cpe:2.3:h:7-eleven:led_message_cup:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2023-34761 : An unauthenticated attacker within BLE proximity can remotely connect to a 7-Eleven LED Message Cu… twitter.com/i/web/status/1…	2023-06-28 20:03:08

← Previous ID

Next ID→