



CVE-2022-28799

Published on: Not Yet Published

Last Modified on: 12/09/2022 07:33:00 PM UTC

CVE-2022-28799

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

Certain versions of [TikTok](#) from [TikTok](#) contain the following vulnerability:

The TikTok application before 23.7.3 for Android allows account takeover. A crafted URL (unvalidated deeplink) can force the com.zhiliaoapp.musically WebView to load an arbitrary website. This may allow an attacker to leverage an attached JavaScript interface for the takeover with one click.

CVE-2022-28799 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

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

CVSS2 Score: **6.8 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Report security vulnerabilities TikTok Help Center	support.tiktok.com/text/html	MISC support.tiktok.com/en/safety-hc/reporting-security-vulnerabilities/reporting-the-security-vulnerabilities

Direct Request ('Forced Browsing') in com.zhiliaapp.musically can lead to user account hijacking · Advisory · Ch0pin/security-advisories · GitHub

github.com
text/html

MISC github.com/Ch0pin/security-advisories/security/advisories/GHSA-v39p-88q5-5cvr

HackerOne

hackerone.com
text/html

MISC hackerone.com/reports/1500614

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.

Related QID Numbers

630810 TikTok For Android Remote Code Execution (RCE) Vulnerability

Exploit/POC from Github

This repository contains a collection of data files on known Common Vulnerabilities and Exposures (CVEs). Each file i...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tiktok	Tiktok	All	All	All	All
cpe:2.3:a:tiktok:tiktok:*:*:*:*:android:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @ipssignatures	The vuln CVE-2022-28799 has a tweet created 0 days ago and retweeted 10 times. twitter.com/CVEnew/status/... #pow1rtrwwcve	2022-05-31 02:06:00
 @RedPacketSec	TikTok account hijacking CVE-2022-28799 - redpacketsecurity.com/tiktok-account...	2022-06-01 09:01:34
 @CVEreport	CVE-2022-28799 : The TikTok application before 23.8.4 for Android allows account takeover. A crafted URL unvalidat... twitter.com/i/web/status/1...	2022-06-02 13:56:01
 /r/hacking	Microsoft researchers discovered a high-severity flaw (CVE-2022-28799) in the TikTok Android app, which could have allowed attackers to hijack users' accounts with a single click	2022-09-01 03:31:41
 /r/RedSec	Microsoft researchers discovered a high-severity flaw (CVE-2022-28799) in the TikTok Android app, which could have allowed attackers to hijack users' accounts with a single click	2022-09-01 17:43:02

← Previous ID

Next ID →

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](#)