CVE-2023-36620

Published on: Not Yet Published

Last Modified on: 11/03/2023 01:22:00 PM UTC

CVE-2023-36620

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

The following vulnerability was found:

An issue was discovered in the Boomerang Parental Control application before 13.83 for Android. The app is missing the android:allowBackup="false" attribute in the manifest. This allows the user to backup the internal memory of the app to a PC. This gives the user access to the API token that is used to authenticate requests to the API.

CVE-2023-36620 has been assigned by cve@mitre.org to track the vulnerability

CVE References

Description	Tags	Link
The hidden costs of parental control apps - SEC Consult	sec-consult.com text/html	MISC sec-consult.com/blog/detail/the-hidden-costs-of-parental-control-apps/
Full Disclosure: SEC Consult SA-20230628-0 :: Stored XSS & Privilege Escalation in Boomerang Parental Control App	seclists.org text/html	MISC seclists.org/fulldisclosure/2023/Jul/12
Boomerang Parental Control - Taking the battle out of screen time	useboomerang.com text/html	MISC useboomerang.com/

There are currently no QIDs associated with this CVE

There are no known software configurations (CPEs) currently associated with this CVE

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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