  - Risk Management
  - Compliance
  - Privacy
  - Supply Chain
- Security Architecture
  - Cloud Security
  - Identity & Access
  - Data Protection
  - Network Security
  - Application Security
- Security Strategy
  - Risk Management
  - Security Architecture
  - Disaster Recovery
  - Training & Certification
  - Incident Response
- ICS/OT
- IoT Security

Home › Mobile Security

# Audio Codec Made by Apple Introduced Serious Vulnerabilities in Millions of Android Phones

By Eduard Kovacs on April 22, 2022

Share 发推 推荐 15 RSS

**An open source audio codec developed by Apple is affected by serious vulnerabilities that have been pushed to millions of Android devices by some of the world's largest mobile chipset manufacturers.**

The Apple Lossless Audio Codec (ALAC) was introduced by Apple in 2004 and, in 2011, the tech giant decided to make ALAC open source. The open source ALAC code has been picked up by many other vendors for non-Apple devices.

Apple has continued to improve the proprietary version of the codec, but the open source code has never been updated in the past 11 years and it seems that the third-party vendors using that code have not made efforts to ensure it's secure.

Researchers at cybersecurity firm Check Point discovered that the open source ALAC code is affected by serious vulnerabilities, and at least two major mobile chipset makers — Qualcomm and MediaTek — have used it for their audio decoders.

Qualcomm and MediaTek have significant market shares and Check Point believes that millions of smartphones worldwide were made vulnerable to attacks due to the use of the ALAC codec.

The security firm estimates that the flaws found by its researchers — the vulnerabilities have been dubbed ALHACK — put roughly two-thirds of Android users' privacy at risk.

The vulnerabilities can be triggered using specially crafted audio files and they can lead to remote code execution.

"The impact of an RCE vulnerability can range from malware execution to an attacker gaining control over a user's multimedia data, including streaming from a compromised machine's camera," Check Point explained in a blog post published on Thursday. "In addition, an unprivileged Android app could use these vulnerabilities to escalate its privileges and gain access to media data and user conversations."

The MediaTek vulnerabilities, patched in December 2021, are identified as CVE-2021-0675 and CVE-2021-0674 and they have been assigned "high" and "medium" severity ratings. Qualcomm also released patches in December 2021. The Qualcomm flaw is tracked as CVE-2021-30351 and it has been assigned a "critical" severity rating.

Check Point plans on disclosing technical details next month at the CanSecWest conference.

**Related:** Google Patches Android Zero-Day Exploited in Targeted Attacks

**Related:** 44 Vulnerabilities Patched in Android With April 2022 Security Updates

Share 发推 推荐 15 RSS

Eduard Kovacs (@EduardKovacs) is a contributing editor at SecurityWeek. He worked as a high school IT teacher for two years before starting a career in journalism as Softpedia's security news reporter. Eduard holds a bachelor's degree in industrial informatics and a master's degree in computer techniques applied in electrical engineering.
Previous Columns by Eduard Kovacs:
Motorola Launches Cyber Threat Information Sharing Hub for Public Safety
Several Critical Vulnerabilities Affect SmartPTT, SmartICS Industrial Products
Unpatched Vulnerability Allows Hackers to Steal Emails of RainLoop Users
Audio Codec Made by Apple Introduced Serious Vulnerabilities in Millions of Android Phones
ICS Exploits Earn Hackers $400,000 at Pwn2Own Miami 2022

**Tags:**
Mobile Security NEWS & INDUSTRY Vulnerabilities Mobile & Wireless

Search

## Get the Daily Briefing

BRIEFING