MX Player Android App Directory Traversal

High

← View More Research Advisories

Synopsis

CVE-2020-5764 - Directory Traversal (RCE)

The MX Transfer protocol is vulnerable to directory traversal in versions below v1.24.5. If a victim enables MX Share as a receiver, an attacker can abuse the sharing protocol by sending a *MessageType* of "*FILE_LIST*" with a "name" field containing directory traversal characters (../). This will result in the file being transferred to the victim's phone, but being saved outside of the intended "/sdcard/MXshare" directory. In our testing, we found we could achieve remote code execution on some Android phones if the attacker sends a "../../../../../data/data/com.mxtech.videoplayer.ad/files/oat/arm64/audience_network.odex" file and "../../../../../data/data/com.mxtech.videoplayer.ad/files/oat/arm64/audience_network.vdex" file with appropriate payloads in order to gain code execution upon next time the app is started by the victim.

Solution

Update to version MX Player v1.24.5 or higher

Proof of Concept

https://github.com/tenable/poc/blob/master/MXPlayer/

Disclosure Timeline

4/9/2020 - Tenable reaches out to support@mxplayer.in, to ask for security contact.
4/10/2020 - MX Player Support asks for disclosure.
4/12/2020 - Tenable discloses vulnerabilities to MX Player Support.
4/13/2020 - MX Player Support acknowledges disclosure report and says development and security teams are working on a fix.
4/27/2020 - Tenable follows up, asking for expected release date for fix.
5/15/2020 - Tenable follows up asking for update.
6/22/2020 - Tenable asks for update, reminds disclosure date is coming soon.
7/6/2020 - Tenable discovers patch in MX Player version fix in v1.24.5

Risk Information

CVE ID: CVE-2020-5764
Tenable Advisory ID: TRA-2020-41
Credit: David Wells

CVSSv2 Base / Temporal Score: 7.3
CVSSv2 Vector: AV:A/AC:L/Au:N/C:P/I:P/A:C
Risk Factor: High

Advisory Timeline

07-07-2020 - Initial Release

FEATURED SOLUTIONS

Application Security
Building Management Systems
Cloud Security Posture Management
Compliance
Exposure Management
Finance
Healthcare
IT/OT
Ransomware
State / Local / Education
US Federal
Vulnerability Management
Zero Trust
→ View all Solutions

CUSTOMER RESOURCES

Resource Library
Community & Support
Customer Education
Tenable Research
Documentation
Trust and Assurance
Nessus Resource Center
Cyber Exposure Fundamentals
System Status

CONNECTIONS

Blog
Contact Us
Careers
Investors
Events
Media