Dolby

Dolby Security Advisory

Dolby Digital Plus – UDC

Summary Description

An out of bounds write within UDC v4.5 -> UDC v4.13 may occur when a unique Dolby Digital Plus (DD+) bitstream is processed by a DD+ decoder. This issue does not occur with a standard DD+ bitstream but only when a manually edited (though "valid") bitstream is created. Dolby authoring tools are incapable of creating this type of bitstream.

We are aware of a report found with Google Pixel devices indicating that there is a possible increased risk of vulnerability if this bug is used alongside other known Pixel vulnerabilities. Other Android mobile devices could be at risk of similar vulnerabilities.

For other device classes, we believe the risk of using this bug maliciously is low and the most commonly observed outcome is a media player crash or restart.

Component: UDC
Vulnerability type: Integer Overflow
Impact: Code Execution
CVSS 3.1 Overall Score: 6.7
Severity: Medium
CVE: CVE-2025-54957

OEM Mitigation Strategy:

OEMs and component providers with products that incorporate DD+ should contact their Dolby representative for information regarding the most up to date Dolby Digital Plus deliverables.

Consumer Mitigation Strategy:

Consumers are recommended to ensure that devices are kept up to date. When supported, we recommend enabling automatic updates so that the most recent software is installed automatically. For specific device inquiries, consumers should reach out to the original device manufacturer.

Acknowledgement:

Dolby would like to thank Ivan Fratric and Natalie Silvanovich of Google Project Zero for identifying this issue and working with Dolby.