



CVE-2017-0807

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2017-0807
State	PUBLIC
Assigner	security@android.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-10-04 01:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	An elevation of privilege vulnerability in the Android framework (ui framework). Product: Android. Versions: 4.4.4, 5.0.2, 5.1.

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Google	Android	4.4.4	All	All	All
Operating System	Google	Android	5.0.2	All	All	All
Operating System	Google	Android	5.1.1	All	All	All
Operating System	Google	Android	6.0	All	All	All
Operating System	Google	Android	6.0.1	All	All	All
Operating System	Google	Android	7.0	All	All	All
Operating System	Google	Android	7.1.1	All	All	All
Operating System	Google	Android	7.1.2	All	All	All
Operating System	Google	Android	4.4.4	All	All	All
Operating System	Google	Android	5.0.2	All	All	All
Operating System	Google	Android	5.1.1	All	All	All
Operating System	Google	Android	6.0	All	All	All
Operating System	Google	Android	6.0.1	All	All	All
Operating System	Google	Android	7.0	All	All	All
Operating System	Google	Android	7.1.1	All	All	All
Operating System	Google	Android	7.1.2	All	All	All

References				
Reference	Source	Link	Tags	
Android Security Bulletin—December 2017 Android Open Source Project	CONFIRM	source.android.com	Vendor	
Google Android Media Framework Multiple Security Vulnerabilities	BID	www.securityfocus.com	Third	
Google Android Framework Multiple Privilege Escalation Vulnerabilities	BID	www.securityfocus.com	Third	
Pixel / Nexus Security Bulletin—October 2017 Android Open Source Project	CONFIRM	source.android.com	Vendor	
CVE Program record	CVE.ORG	www.cve.org	canonical	
NVD vulnerability detail	NVD	nvd.nist.gov	canonical	
No vendor comments have been submitted for this CVE.				
There are currently no legacy QID mappings associated with this CVE.				