



CVE-2016-3744

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

Summary	
CVE	CVE-2016-3744
State	PUBLISHED
Assigner	google_android
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-07-11 01:59:44 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Buffer overflow in the create_pbuf function in btif/src/btif_hh.c in Bluetooth in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.

Risk And Classification

Primary CVSS: v3.0 7.5 HIGH from nvd@nist.gov

CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Problem Types: CWE-119 | CWE-362 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	7.5	HIGH	CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	4.3		AV:A/AC:H/Au:N/C:P/I:P/A:P

CVSS v3.0 Breakdown	
Attack Vector	Adjacent
Attack Complexity	High
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	

High

CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Adjacent

Access Complexity

High

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:A/AC:H/Au:N/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Google	Android	4.0	All	All	All
Operating System	Google	Android	4.0.1	All	All	All
Operating System	Google	Android	4.0.2	All	All	All
Operating System	Google	Android	4.0.3	All	All	All
Operating System	Google	Android	4.0.4	All	All	All
Operating System	Google	Android	4.1	All	All	All
Operating System	Google	Android	4.1.2	All	All	All
Operating System	Google	Android	4.2	All	All	All
Operating System	Google	Android	4.2.1	All	All	All
Operating System	Google	Android	4.2.2	All	All	All
Operating System	Google	Android	4.3	All	All	All
Operating System	Google	Android	4.3.1	All	All	All
Operating System	Google	Android	4.4	All	All	All
Operating System	Google	Android	4.4.1	All	All	All
Operating System	Google	Android	4.4.2	All	All	All
Operating System	Google	Android	4.4.3	All	All	All
Operating System	Google	Android	5.0	All	All	All

Operating System	Google	Android	5.0.1	All	All	All
Operating System	Google	Android	5.1	All	All	All
Operating System	Google	Android	5.1.0	All	All	All
Operating System	Google	Android	6.0	All	All	All
Operating System	Google	Android	6.0.1	All	All	All

Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		

References			
Reference	Source		Link
Android Security Bulletin—July 2016 Android Open Source Project	af854a3a-2127-422b-91ae-364da2661108		source.a
514139f4b40cbb035bb92f3e24d5a389d75db9e6 - platform/system/bt - Git at Google	af854a3a-2127-422b-91ae-364da2661108		android.g
CVE Program record	CVE.ORG		www.cve
NVD vulnerability detail	NVD		nvd.nist.g

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.