



CVE-2016-0843

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

Summary	
CVE	CVE-2016-0843
State	PUBLISHED
Assigner	google_android
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-04-18 00:59:08 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The Qualcomm ARM processor performance-event manager in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 5.2.x before 5.2.1 contains a buffer overflow in the <code>pmem_event_manager</code> function. A remote attacker could exploit this vulnerability to cause a denial of service or execute arbitrary code on the affected device. CVE-2016-0843 is a <code>Buffer Overflow</code> in the <code>pmem_event_manager</code> function in the <code>pmem</code> component of the Qualcomm ARM processor performance-event manager in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 5.2.x before 5.2.1. A remote attacker could exploit this vulnerability to cause a denial of service or execute arbitrary code on the affected device. CVE-2016-0843 is a <code>Buffer Overflow</code> in the <code>pmem_event_manager</code> function in the <code>pmem</code> component of the Qualcomm ARM processor performance-event manager in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 5.2.x before 5.2.1. A remote attacker could exploit this vulnerability to cause a denial of service or execute arbitrary code on the affected device.

Risk And Classification

Primary CVSS: v3.0 8.4 HIGH from nvd@nist.gov

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

Problem Types: CWE-264 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	8.4	HIGH	CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	7.2		AV:L/AC:L/Au:N/C:C/I:C/A:C

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

High

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

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:L/AC:L/Au:N/C:C/I:C/A:C

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	Tag
Nexus Security Bulletin—April 2016 Android Open Source Project	af854a3a-2127-422b-91ae-364da2661108		source.android.com	Patc
CVE Program record	CVE.ORG		www.cve.org	canc
NVD vulnerability detail	NVD		nvd.nist.gov	canc

No vendor comments have been submitted for this CVE.

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