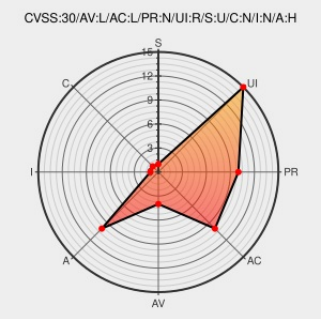
CVE-2017-5217

Published on: 01/09/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:48 PM UTC

CVE-2017-5217

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Samsung Mobile from Samsung contain the following vulnerability:

Installing a zero-permission Android application on certain Samsung Android devices with KK(4.4), L(5.0/5.1), and M(6.0) software can continually crash the system_server process in the Android OS. The zero-permission app will create an active install session for a separate app that it has embedded within it. The active install session of the embedded app is performed using the android.content.pm.PackageInstaller class and its nested classes in the Android API. The active install session will write the embedded APK file to the /data/app directory, but the app will not be installed since third-party applications cannot programmatically install apps. Samsung has modified AOSP in order to accelerate the parsing of APKs by introducing the com.android.server.pm.PackagePrefetcher class and its nested classes. These classes will parse the APKs present in the /data/app directory and other directories, even if the app is not actually installed. The embedded APK that was written to the /data/app directory via the active install session has a very large but valid AndroidManifest.xml file. Specifically, the AndroidManifest.xml file contains a very large string value for the name of a permission-tree that it declares. When system_server tries to parse the APK file of the embedded app from the active install session, it will crash due to an uncaught error (i.e., java.lang.OutOfMemoryError) or an uncaught exception (i.e., std::bad_alloc) because of memory constraints. The Samsung Android device will encounter a soft reboot due to a system_server crash, and this action will keep repeating since parsing the APKs in the /data/app directory as performed by the system_server process is part of the normal boot process. The Samsung ID is SVE-2016-6917.

CVE-2017-5217 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.5 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED

Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: 7.1 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE

Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	COMPLETE

CVE References

Description	Tags	Link
Multiple Samsung Android Mobile Phones CVE-2017-5217 Denial of Service Vulnerability	cve.report (archive) text/html	BID 95319
Error Message | SAMSUNG Mobile Security	Vendor Advisory security.samsungmobile.com text/html	CONFIRM security.samsungmobile.com/smrupdate.html#SMR-JAN-2017

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Samsung	Samsung Mobile	4.4	All	All	All
Operating System	Samsung	Samsung Mobile	5.0	All	All	All
Operating System	Samsung	Samsung Mobile	5.1	All	All	All
Operating System	Samsung	Samsung Mobile	6.0	All	All	All
Operating System	Samsung	Samsung Mobile	4.4	All	All	All
Operating System	Samsung	Samsung Mobile	5.0	All	All	All
Operating System	Samsung	Samsung Mobile	5.1	All	All	All
Operating System	Samsung	Samsung Mobile	6.0	All	All	All

cpe:2.3:o:samsung:samsung_mobile:4.4:*:*:*:*:*:*:*

cpe:2.3:o:samsung:samsung_mobile:5.0:*:*:*:*:*:*:*

cpe:2.3:o:samsung:samsung_mobile:5.1:*:*:*:*:*:*:*

cpe:2.3:o:samsung:samsung_mobile:6.0:*:*:*:*:*:*:*

cpe:2.3:o:samsung:samsung_mobile:4.4:*:*:*:*:*:*:*

cpe:2.3:o:samsung:samsung_mobile:5.0:*:*:*:*:*:*:*

cpe:2.3:o:samsung:samsung_mobile:5.1:*:*:*:*:*:*:*

cpe:2.3:o:samsung:samsung_mobile:6.0:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→