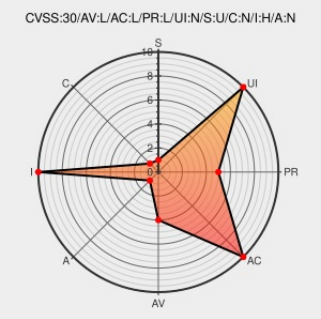
CVE-2018-14992

Published on: 12/28/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:43 PM UTC

CVE-2018-14992

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



Certain versions of Zenfone 3 Max from Asus contain the following vulnerability:

The ASUS ZenFone 3 Max Android device with a build fingerprint of asus/US_Phone/ASUS_X008_1:7.0/NRD90M/US_Phone-14.14.1711.92-20171208:user/release-keys contains a pre-installed platform app with a package name of com.asus.dm (versionCode=1510500200, versionName=1.5.0.40_171122) has an exposed interface in an exported service named com.asus.dm.installer.DMInstallerService that allows any app co-located on the device to use its capabilities to download an arbitrary app over the internet and install it. Any app on the device can send an intent with specific embedded data that will cause the com.asus.dm app to programmatically download and install the app. For the app to be downloaded and installed, certain data needs to be provided: download URL, package name, version name from the app's AndroidManifest.xml file, and the MD5 hash of the app. Moreover, any app that is installed using this method can also be programmatically uninstalled using the same unprotected component named com.asus.dm.installer.DMInstallerService.

CVE-2018-14992 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	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	HIGH	NONE

CVSS2 Score: 2.1 - LOW

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE

Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Page not found | Kryptowire	Exploit Vendor Advisory www.kryptowire.com application/pdf Inactive Link Not Archived	MISC www.kryptowire.com/portal/wp-content/uploads/2018/12/DEFCON-26-Johnson-and-Stavrou-Vulnerable-Out-of-the-Box-An-Eval-of-Android-Carrier-Devices-WP-Updated.pdf
Kryptowire Provides Details on DEFCON 2018 Presentation: Vulnerable Out of the Box - An Evaluation of Android Carrier Devices - Kryptowire	Vendor Advisory www.kryptowire.com text/html	MISC www.kryptowire.com/portal/android-firmware-defcon-2018/

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Asus	Zenfone 3 Max	-	All	All	All
Hardware	Asus	Zenfone 3 Max	-	All	All	All
Operating System	Asus	Zenfone 3 Max Firmware	1.5.0.40	All	All	All
Operating System	Asus	Zenfone 3 Max Firmware	1.5.0.40	All	All	All

cpe:2.3:h:asus:zenfone_3_max:-:*:*:*:*:*:*:*:

cpe:2.3:h:asus:zenfone_3_max:-:*:*:*:*:*:*:*:

cpe:2.3:o:asus:zenfone_3_max_firmware:1.5.0.40:*:*:*:*:*:*:*:

cpe:2.3:o:asus:zenfone_3_max_firmware:1.5.0.40:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report