

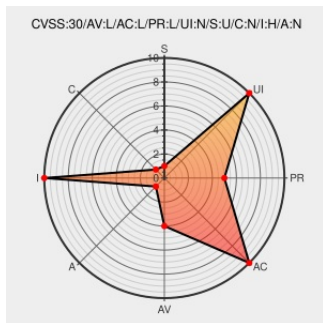


CVE-2018-14992

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 [M](#) 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

NONE

Integrity Impact

PARTIAL

Availability Impact

NONE

CVE References

Description

Page not found | Kryptowire

Tags

Exploit

Vendor Advisory

www.kryptowire.com

application/pdf

Inactive Link

Not Archived

Link

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

Description

Kryptowire Provides Details on DEFCON 2018 Presentation: Vulnerable Out of the Box - An Evaluation of Android Carrier Devices - Kryptowire

Tags

Vendor Advisory

www.kryptowire.com

text/html

Link

MISC

www.kryptowire.com/portal/android-firmware-defcon-2018/

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type

Hardware

Hardware

Operating System

Operating System

Vendor

Asus

Asus

Asus

Asus

Product

Zenfone 3 Max

Zenfone 3 Max

Zenfone 3 Max Firmware

Zenfone 3 Max Firmware

Version

-

-

1.5.0.40

1.5.0.40

Update

All

All

All

All

Edition

All

All

All

All

Language

All

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 →

completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)