



CVE-2018-14994

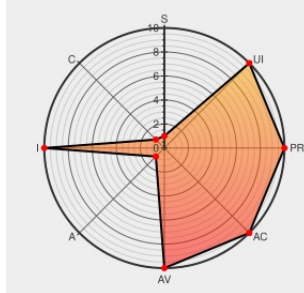
Published on: 04/25/2019 12:00:00 AM UTC

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

CVE-2018-14994

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:30/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N



Certain versions of [Phone](#) from [Essential](#) contain the following vulnerability:

The Essential Phone Android device with a build fingerprint of essential/mata/mata:8.1.0/OPM1.180104.166/297:user/release-keys contains a pre-installed platform app with a package name of com.ts.android.hiddenmenu (versionName=1.0, platformBuildVersionName=8.1.0) that contains an exported activity

app component named com.ts.android.hiddenmenu.rtn.RTNResetActivity that allows any app co-located on the device to programmatically initiate a factory reset. In addition, the app initiating the factory reset does not require any permissions. A factory reset will remove all user data and apps from the device. This will result in the loss of any data that have not been backed up or synced externally. The capability to perform a factory reset is not directly available to third-party apps (those that the user installs themselves with the exception of enabled Mobile Device Management (MDM) apps), although this capability can be obtained by leveraging an unprotected app component of a pre-installed platform app.

CVE-2018-14994 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	HIGH	NONE

CVSS2 Score: **9.4 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality	Integrity	Availability

Impact	Impact	Impact
NONE	COMPLETE	COMPLETE

CVE References		
Description	Tags	Link
Homepage Kryptowire	Third Party Advisory www.kryptowire.com text/html	Q MISC www.kryptowire.com
Page not found Kryptowire	Third Party Advisory www.kryptowire.com application/pdf Inactive Link Not Archived	Q 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	Exploit Third Party Advisory www.kryptowire.com text/html	Q 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	Vendor	Product	Version	Update	Edition	Language
Hardware	Essential	Phone	-	All	All	All
Hardware	Essential	Phone	-	All	All	All
Operating System	Essential	Phone Firmware	-	All	All	All
Operating System	Essential	Phone Firmware	-	All	All	All
cpe:2.3:h:essential:phone:-:*:*:*:*:*:						
cpe:2.3:h:essential:phone:-:*:*:*:*:*:						
cpe:2.3:o:essential:phone_firmware:-:*:*:*:*:*:						
cpe:2.3:o:essential:phone_firmware:-:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, 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](#)