

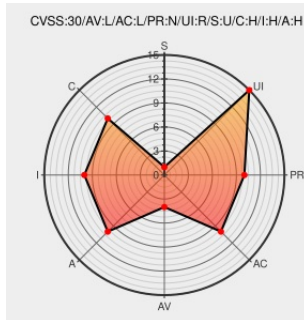


CVE-2017-8160

Published on: 11/22/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:43 PM UTC

CVE-2017-8160

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

Certain versions of [Vicky-al00a](#) from [Huawei](#) contain the following vulnerability:

The Madapt Driver of some Huawei smart phones with software Earlier than Vicky-AL00AC00B172 versions, Vicky-AL00CC768B122, Vicky-TL00AC01B167, Earlier than Victoria-AL00AC00B172 versions, Victoria-TL00AC00B123, Victoria-TL00AC01B167 has a use after free (UAF) vulnerability. An attacker can trick a user to install a malicious application which has a high privilege to exploit this vulnerability, Successful exploitation may cause arbitrary code execution.

CVE-2017-8160 has been assigned by psirt@huawei.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: Huawei Technologies Co., Ltd. - Vicky-AL00A, Vicky-AL00C, Vicky-TL00A, Victoria-AL00A, Victoria-TL00A version Earlier than Vicky-AL00AC00B172 versions, Vicky-AL00CC768B122, Vicky-TL00AC01B167, Earlier than Victoria-AL00AC00B172 versions, Victoria-TL00AC00B123, Victoria-TL00AC01B167

CVSS3 Score: **7.8 - HIGH**

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

CVSS2 Score: **9.3 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description

Tags

Link

Security Advisory - Use After Free Vulnerability in Madapt Driver of Some Huawei Smart Phones

Vendor Advisory
www.huawei.com
text/html

 CONFIRM www.huawei.com/en/psirt/security-advisories/huawei-sa-20171018-01-smartphone-en

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 	Huawei	Vicky-al00a	-	All	All	All
Hardware 	Huawei	Vicky-al00a	-	All	All	All
Operating System	Huawei	Vicky-al00a Firmware	All	All	All	All
Operating System	Huawei	Vicky-al00a Firmware	All	All	All	All
Hardware 	Huawei	Vicky-al00c	-	All	All	All
Hardware 	Huawei	Vicky-al00c	-	All	All	All
Operating System	Huawei	Vicky-al00c Firmware	vicky-al00cc768b122	All	All	All
Operating System	Huawei	Vicky-al00c Firmware	vicky-al00cc768b122	All	All	All
Hardware 	Huawei	Vicky-tl00a	-	All	All	All
Hardware 	Huawei	Vicky-tl00a	-	All	All	All
Operating System	Huawei	Vicky-tl00a Firmware	vicky-tl00ac01b167	All	All	All
Operating System	Huawei	Vicky-tl00a Firmware	vicky-tl00ac01b167	All	All	All
Hardware 	Huawei	Victoria-al00a	-	All	All	All
Hardware 	Huawei	Victoria-al00a	-	All	All	All
Operating System	Huawei	Victoria-al00a Firmware	All	All	All	All
Operating System	Huawei	Victoria-al00a Firmware	All	All	All	All
Hardware 	Huawei	Victoria-tl00a	-	All	All	All
Hardware 	Huawei	Victoria-tl00a	-	All	All	All

Operating System	Huawei	Victoria-tl00a Firmware	victoria-tl00ac00b123	All	All	All
Operating System	Huawei	Victoria-tl00a Firmware	victoria-tl00ac01b167	All	All	All
Operating System	Huawei	Victoria-tl00a Firmware	victoria-tl00ac00b123	All	All	All
Operating System	Huawei	Victoria-tl00a Firmware	victoria-tl00ac01b167	All	All	All
cpe:2.3:h:huawei:vicky-al00a:-:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:h:huawei:vicky-al00a:-:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:huawei:vicky-al00a_firmware:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:huawei:vicky-al00a_firmware:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:h:huawei:vicky-al00c:-:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:h:huawei:vicky-al00c:-:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:huawei:vicky-al00c_firmware:vicky-al00cc768b122:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:huawei:vicky-al00c_firmware:vicky-al00cc768b122:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:h:huawei:vicky-tl00a:-:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:h:huawei:vicky-tl00a:-:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:huawei:vicky-tl00a_firmware:vicky-tl00ac01b167:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:huawei:vicky-tl00a_firmware:vicky-tl00ac01b167:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:h:huawei:victoria-al00a:-:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:h:huawei:victoria-al00a:-:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:huawei:victoria-al00a_firmware:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:huawei:victoria-al00a_firmware:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:h:huawei:victoria-tl00a:-:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:h:huawei:victoria-tl00a:-:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:huawei:victoria-tl00a_firmware:victoria-tl00ac00b123:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:huawei:victoria-tl00a_firmware:victoria-tl00ac01b167:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:huawei:victoria-tl00a_firmware:victoria-tl00ac00b123:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:huawei:victoria-tl00a_firmware:victoria-tl00ac01b167:~::~~::~~::~~::~~::~~::~~::						

No vendor comments have been submitted for this CVE

© CVE.report 2023   |

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](#)