



CVE-2017-8173

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

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

CVE-2017-8173

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

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



Certain versions of [Maya-L02](#) from [Huawei](#) contain the following vulnerability:

Maya-L02,VKY-L09,VTR-L29,Vicky-AL00A,Victoria-AL00A,Warsaw-AL00 smart phones with software of earlier than Maya-L02C636B126 versions,earlier than VKY-L29C10B151 versions,earlier than VTR-L29C10B151 versions,earlier than Vicky-AL00AC00B162 versions,earlier than Victoria-AL00AC00B167 versions,earlier than

Warsaw-AL00C00B200 versions have a Factory Reset Protection (FRP) bypass security vulnerability. When re-configuring the mobile phone using the factory reset protection (FRP) function, an attacker can login the configuration flow by some secret code and can perform some operations to update the Google account. As a result, the FRP function is bypassed.

CVE-2017-8173 has been assigned by psirt@huawei.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: Huawei Technologies Co., Ltd. - Maya-L02,VKY-L09,VTR-L29,Vicky-AL00A,Victoria-AL00A,Warsaw-AL00 version Earlier than Maya-L02C636B126 versions,Earlier than VKY-L29C10B151 versions,Earlier than VTR-L29C10B151 versions,Earlier than Vicky-AL00AC00B162 versions,Earlier than Victoria-AL00AC00B167 versions,Earlier than Warsaw-AL00C00B200 versions

CVSS3 Score: **4.6 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
PHYSICAL	LOW	NONE	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

impact	impact	impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Security Advisory - FRP Bypass Vulnerability in Huawei Smart Phones	Issue Tracking Vendor Advisory www.huawei.com text/html	 CONFIRM www.huawei.com/en/psirt/security-advisories/huawei-sa-20170715-01-frpbypass-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	Maya-I02	-	All	All	All
Hardware 	Huawei	Maya-I02	-	All	All	All
Operating System	Huawei	Maya-I02 Firmware	All	All	All	All
Operating System	Huawei	Maya-I02 Firmware	All	All	All	All
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	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	Vky-I09	-	All	All	All
Hardware 	Huawei	Vky-I09	-	All	All	All
Operating System	Huawei	Vky-I09 Firmware	All	All	All	All
Operating System	Huawei	Vky-I09 Firmware	All	All	All	All

system

Hardware		Huawei	Vky-l29	-	All	All	All
Hardware		Huawei	Vky-l29	-	All	All	All
Operating System		Huawei	Vky-l29 Firmware	All	All	All	All
Operating System		Huawei	Vky-l29 Firmware	All	All	All	All
Hardware		Huawei	Warsaw-al00	-	All	All	All
Hardware		Huawei	Warsaw-al00	-	All	All	All
Operating System		Huawei	Warsaw-al00 Firmware	All	All	All	All
Operating System		Huawei	Warsaw-al00 Firmware	All	All	All	All
cpe:2.3:h:huawei:maya-l02:-:~::~:							
cpe:2.3:h:huawei:maya-l02:-:~::~:							
cpe:2.3:o:huawei:maya-l02_firmware:~::~:							
cpe:2.3:o:huawei:maya-l02_firmware:~::~:							
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: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:vky-l09:-:~::~:							
cpe:2.3:h:huawei:vky-l09:-:~::~:							
cpe:2.3:o:huawei:vky-l09_firmware:~::~:							
cpe:2.3:o:huawei:vky-l09_firmware:~::~:							
cpe:2.3:h:huawei:vky-l29:-:~::~:							
cpe:2.3:h:huawei:vky-l29:-:~::~:							
cpe:2.3:o:huawei:vky-l29_firmware:~::~:							

cpe:2.3:o:huawei:vky-l29_firmware:*:*:*:*:*:
cpe:2.3:h:huawei:warsaw-al00-*:*:*:*:*:
cpe:2.3:h:huawei:warsaw-al00-*:*:*:*:*:
cpe:2.3:o:huawei:warsaw-al00_firmware:*:*:*:*:*:
cpe:2.3:o:huawei:warsaw-al00_firmware:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →