

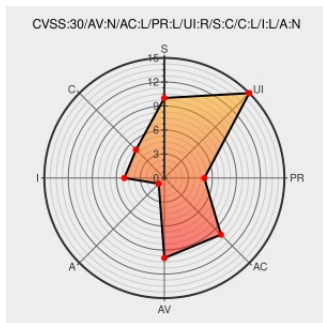


CVE-2017-8178

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

Last Modified on: 03/23/2021 11:26:42 PM UTC

CVE-2017-8178

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

Certain versions of [Vicky-al00](#) from [Huawei](#) contain the following vulnerability:

Huawei Email APP Vicky-AL00 smartphones with software of earlier than VKY-AL00C00B171 versions has a stored cross-site scripting vulnerability. A remote attacker could exploit this vulnerability to send email that storing malicious code to a smartphone and waiting for a user to access this email that triggers execution of the code. An exploit could allow the attacker to execute arbitrary script code on the affected device.

CVE-2017-8178 has been assigned by psirt@huawei.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Huawei Technologies Co., Ltd. - Vicky-AL00** version **Earlier than VKY-AL00C00B171 versions**

CVSS3 Score: **5.4 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	LOW	NONE

CVSS2 Score: **3.5 - LOW**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
-------------	------	------

There are currently no QIDs associated with this CVE

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Huawei	Vicky-al00	-	All	All	All
Hardware	Huawei	Vicky-al00	-	All	All	All
Operating System	Huawei	Vicky-al00 Firmware	All	All	All	All
Operating System	Huawei	Vicky-al00 Firmware	All	All	All	All
<code>cpe:2.3:h:huawei:vicky-al00:-:~::~~::~~::~~::~~::~~::~~:::</code>						
<code>cpe:2.3:h:huawei:vicky-al00:-:~::~~::~~::~~::~~::~~::~~:::</code>						
<code>cpe:2.3:o:huawei:vicky-al00_firmware:*:*:*:*:*::~~::~~::~~::~~::~~::~~::~~:::</code>						
<code>cpe:2.3:o:huawei:vicky-al00_firmware:*:*:*:*:*::~~::~~::~~::~~::~~::~~::~~:::</code>						

Next ID→