



CVE-2017-2882

Published on: 11/07/2017 12:00:00 AM UTC

Last Modified on: 06/03/2022 07:06:00 PM UTC

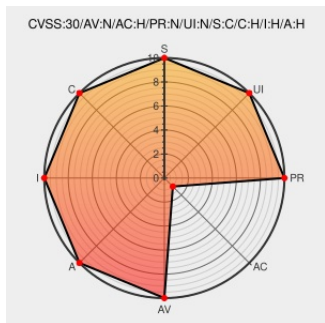
CVE-2017-2882

Source: [Mitre](#)

Source: [NIST](#)

[CVE.ORG](#)

Print: [PDF](#)



Certain versions of [Circle With Disney](#) from [Meetcircle](#) contain the following vulnerability:

An exploitable vulnerability exists in the servers update functionality of Circle with Disney running firmware 2.0.1. Specially crafted network packets can cause the device to overwrite sensitive files, resulting in code execution. An attacker needs to impersonate a remote server in order to trigger this vulnerability.

CVE-2017-2882 has been assigned by [talos-cna@cisco.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [Cisco](#) **Circle Media** - **Circle** version **firmware 2.0.1**

CVSS3 Score: **8.1 - HIGH**

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

CVSS2 Score: **6.8 - MEDIUM**

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

CVE References

Description	Tags	Link
TALOS-2017-0389 Cisco Talos Intelligence Group -	Exploit	MISC

There are currently no QIDs associated with this CVE

Type	Vendor	Product	Version	Update	Edition	Language
Hardware 	Meetcircle	Circle With Disney	-	All	All	All
Hardware 	Meetcircle	Circle With Disney	-	All	All	All
Operating System	Meetcircle	Circle With Disney Firmware	2.0.1	All	All	All
Operating System	Meetcircle	Circle With Disney Firmware	2.0.1	All	All	All
cpe:2.3:h:meetcircle:circle_with_disney:-:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:h:meetcircle:circle_with_disney:-:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:meetcircle:circle_with_disney_firmware:2.0.1:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:meetcircle:circle_with_disney_firmware:2.0.1:~::~~::~~::~~::~~::~~::~~:::						