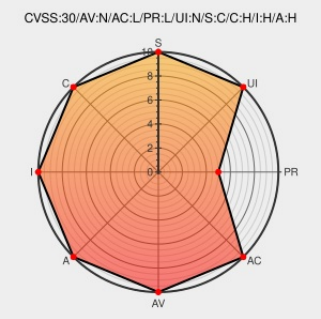
CVE-2017-2898

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

Last Modified on: 06/13/2022 07:17:00 PM UTC

CVE-2017-2898

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 signature verification of the firmware update functionality of Circle with Disney. Specially crafted network packets can cause an unsigned firmware to be installed in the device resulting in arbitrary code execution. An attacker can send a series of packets to trigger this vulnerability.

CVE-2017-2898 has been assigned by talos-cna@cisco.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Circle Media** - **Circle** version **firmware 2.0.1**

CVSS3 Score: 7.5 - HIGH

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

CVSS2 Score: 8.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
TALOS-2017-0405 || Cisco Talos Intelligence Group -	Exploit	MISC

Comprehensive Threat Intelligence	Technical Description Third Party Advisory www.talosintelligence.com text/html	www.talosintelligence.com/vulnerability_reports/TALOS-2017-0405

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→