



CVE-2017-2865

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

Summary	
CVE	CVE-2017-2865
State	PUBLISHED
Assigner	talos
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-11-07 16:29:00 UTC
Updated	2025-04-20 01:37:25 UTC
Description	An exploitable vulnerability exists in the firmware update functionality of Circle with Disney. Specially crafted network packets can be used to trigger a buffer overflow in the update process, leading to a denial of service. The vulnerability is located in the 'fwupdate' utility, which is responsible for updating the device's firmware. The issue is caused by a lack of proper input validation, allowing an attacker to send a large number of malformed packets that overflow the device's memory. This can result in the device becoming unresponsive and requiring a hard reset. The vulnerability is rated as HIGH severity.

Risk And Classification					
Primary CVSS: v3.1 7.5 HIGH from nvd@nist.gov					
CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H					
Problem Types: NVD-CWE-noinfo command injection					
Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7.5	HIGH	CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
3.0	talos-cna@cisco.com	Secondary	9.6	CRITICAL	CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
3.0	CNA	DECLARED	9.6	CRITICAL	CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	7.9		AV:A/AC:M/Au:N/C:C/I:C/A:C

CVSS v3.1 Breakdown	
Attack Vector	Adjacent
Attack Complexity	High
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	High

ntegrity

High

Availability

High

CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.0 Breakdown

Attack Vector

Adjacent

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Changed

Confidentiality

High

ntegrity

High

Availability

High

CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Adjacent

Access Complexity

Medium

Authentication

None

Confidentiality

Complete

ntegrity

Complete

Availability

Complete

AV:A/AC:M/Au:N/C:C/I:C/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Meetcircle	Circle With Disney	-	All	All	All
Operating System	Meetcircle	Circle With Disney Firmware	2.0.1	All	All	All

Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Circle Media	Circle	affected firmware 2.0.1	Not specified		

References				
Reference	Source	Link	Tags	
TALOS-2017-0371 - Cisco Talos	af854a3a-2127-422b-91ae-364da2661108	www.talosintelligence.com	Technical Description, Third Party	
CVE Program record	CVE.ORG	www.cve.org	canonical	
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis	

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report