



CVE-2012-0641

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2012-0641
State	PUBLISHED
Assigner	apple
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-03-08 22:55:04 UTC
Updated	2026-04-29 01:13:23 UTC
Description	CFNetwork in Apple iOS before 5.1 does not properly construct request headers during parsing of URLs, which allows remote attackers to trigger a denial of service via a crafted URL.

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

AV:N/AC:L/Au:N/C:P/I:N/A:N

Problem Types: CWE-20 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

AV:N/AC:L/Au:N/C:P/I:N/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Iphone Os	All	All	All	All

Vendor Declared Affected Products				
Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified
References				
Reference				
About Secunia Research Flexera				
Apple iOS Bugs Let Remote Users Execute Arbitrary Code, Conduct Cross-Site Scripting Attacks, and Obtain Potentially Sensitive Information				
APPLE-SA-2012-03-07-2 iOS 5.1 Software Update				
CVE Program record				
NVD vulnerability detail				
No vendor comments have been submitted for this CVE.				
There are currently no legacy QID mappings associated with this CVE.				