CVE-2013-0962

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

Summary

CVE	CVE-2013-0962
State	PUBLISHED
Assigner	apple
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-01-29 05:58:54 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Cross-site scripting (XSS) vulnerability in WebKit in Apple iOS before 6.1 allows user-assisted remote attackers to inject arb

Risk And Classification

Primary CVSS: v2.0 2.6 from nvd@nist.gov

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

Problem Types: CWE-79 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

High

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Iphone Os	6.0	All	All	All

Operating System	Apple	Iphone Os	6.0.1	All	All	All
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	Source	Link	Tags
APPLE-SA-2013-01-28-1 iOS 6.1 Software Update	af854a3a-2127-422b-91ae-364da2661108	lists.apple.com	Vendor Advisory
About the security content of iOS 6.1 Software Update	af854a3a-2127-422b-91ae-364da2661108	support.apple.com	Vendor Advisory
APPLE-SA-2013-03-14-2 Safari 6.0.3	af854a3a-2127-422b-91ae-364da2661108	lists.apple.com	
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.