CVE-2015-3783

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

Summary

CVE	CVE-2015-3783
State	PUBLISHED
Assigner	apple
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-08-16 23:59:56 UTC
Updated	2026-05-06 22:30:45 UTC
Description	SceneKit in Apple OS X before 10.10.5 allows remote attackers to execute arbitrary code or cause a denial of service (mem

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

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

Problem Types: CWE-119 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference
APPLE-SA-2015-08-13-2 OS X Yosemite v10.10.5 and Security Update 2015-006
About the security content of OS X Yosemite v10.10.5 and Security Update 2015-006 - Apple Support
Apple OS X Multiple Flaws Let Remote Users Execute Arbitrary Code, Obtain Potentially Sensitive Information, and Deny Service and Let Loc
Apple Mac OS X Prior to 10.10.5 Multiple Security Vulnerabilities
Apple qlmanage - SceneKit::daeElement::setElementName Heap Overflow - OSX dos Exploit
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.