



CVE-2014-4406

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

Summary

CVE	CVE-2014-4406
State	PUBLIC
Assigner	product-security@apple.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-09-19 10:55:00 UTC
Updated	2017-09-16 01:29:00 UTC
Description	Cross-site scripting (XSS) vulnerability in Xcode Server in CoreCollaboration in Apple OS X Server before 3.2.1 allows remote attackers to execute arbitrary code via a crafted request.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Os X Server	2.0	All	All	All
Operating System	Apple	Os X Server	2.1	All	All	All
Operating System	Apple	Os X Server	2.1.1	All	All	All
Operating System	Apple	Os X Server	2.2	All	All	All
Operating System	Apple	Os X Server	2.2.1	All	All	All
Operating System	Apple	Os X Server	2.2.2	All	All	All
Operating System	Apple	Os X Server	3.0	All	All	All
Operating System	Apple	Os X Server	3.0.1	All	All	All
Operating System	Apple	Os X Server	3.0.2	All	All	All
Operating System	Apple	Os X Server	3.0.3	All	All	All
Operating System	Apple	Os X Server	3.1	All	All	All
Operating System	Apple	Os X Server	3.1.1	All	All	All
Operating System	Apple	Os X Server	2.0	All	All	All
Operating System	Apple	Os X Server	2.1	All	All	All
Operating System	Apple	Os X Server	2.1.1	All	All	All
Operating System	Apple	Os X Server	2.2	All	All	All
Operating System	Apple	Os X Server	2.2.1	All	All	All

Operating System	Apple	Os X Server	2.2.2	All	All	All
Operating System	Apple	Os X Server	3.0	All	All	All
Operating System	Apple	Os X Server	3.0.1	All	All	All
Operating System	Apple	Os X Server	3.0.2	All	All	All
Operating System	Apple	Os X Server	3.0.3	All	All	All
Operating System	Apple	Os X Server	3.1	All	All	All
Operating System	Apple	Os X Server	3.1.1	All	All	All
Operating System	Apple	Os X Server	All	All	All	All

References

Reference	Source	Link
Apple OS X Server Input Validation Flaw in Xcode Server Permits Cross-Site Scripting Attacks - SecurityTracker	SECTrack	www.securitytracker.com/id?1037211
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com/vulnerabilities/122222
NEOHAPSIS - Peace of Mind Through Integrity and Insight	APPLE	archives.neohapsis.com/archives/apple/000001.html
XSS.CX Blog: CVE-2014-4406, APPLE-SA-2014-09-17-5 OS X Server 3.2.1, DOM XSS, window.location.hash	MISC	www.clouds.tencent.com/2014/09/17/5-os-x-server-3-2-1-dom-xss-window-location-hash/
About the security content of OS X Server v3.2.1 - Apple Support	CONFIRM	support.apple.com/kb/HT201407
About the security content of OS X Server v4.0 - Apple Support	CONFIRM	support.apple.com/kb/HT201407
Security Advisory SA61307 - Apple OS X Server Multiple Vulnerabilities - Secunia	SECUNIA	secunia.com/advisories/61307/apple-os-x-server-multiple-vulnerabilities/
Apple Mac OS X Server CVE-2014-4406 Cross Site Scripting Vulnerability	BID	www.securityfocus.com/bid/68444
CVE Program record	CVE.ORG	www.cve.org/CVE-2014-4406
NVD vulnerability detail	NVD	nvd.nist.gov/vuln/detail/CVE-2014-4406

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://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](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](https://mitre.org/cve).

Free CVE JSON API cve.report/api

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