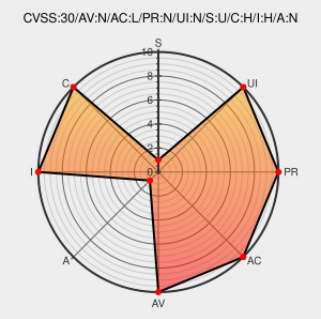
CVE-2016-4694

Published on: 09/25/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:59 PM UTC

CVE-2016-4694

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Mac Os X from Apple contain the following vulnerability:

The Apache HTTP Server in Apple OS X before 10.12 and OS X Server before 5.2 follows RFC 3875 section 4.1.18 and therefore does not protect applications from the presence of untrusted CGI client data in the HTTP_PROXY environment variable, which might allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted Proxy header in an HTTP request, aka an "httpoxy" issue, a related issue to CVE-2016-5387.

CVE-2016-4694 has been assigned by product-security@apple.com to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.1 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	NONE

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
APPLE-SA-2016-09-20-4 macOS Server 5.2	Mailing List	APPLE APPLE-SA-2016

APPLE-SA-2016-09-20-4 macOS Server 5.2	Mailing List Vendor Advisory lists.apple.com text/html	APPLE APPLE-SA-2016-09-20-4
About the security content of macOS Sierra 10.12 - Apple Support	Vendor Advisory support.apple.com text/html	CONFIRM support.apple.com/HT207170
Apple macOS Server "Proxy:" Header Processing Flaw Lets Remote Users Redirect the Target CGI Application Requests to an Arbitrary Web Proxy in Certain Cases - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1036853
APPLE-SA-2016-09-20 macOS Sierra 10.12	Mailing List Vendor Advisory lists.apple.com text/html	APPLE APPLE-SA-2016-09-20
About the security content of macOS Server 5.2 - Apple Support	Vendor Advisory support.apple.com text/html	CONFIRM support.apple.com/HT207171
Apple Mac OS X and Mac OS X Server CVE-2016-4694 Security Bypass Vulnerability	cve.report (archive) text/html	BID 93060

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:o:apple:mac_os_x:*:*:*:*:*:*:*:*:

cpe:2.3:o:apple:os_x_server:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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