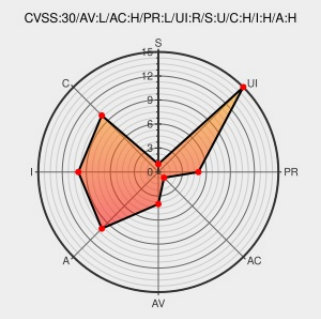
CVE-2015-7024

Published on: 01/11/2016 12:00:00 AM UTC

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

CVE-2015-7024

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



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

Untrusted search path vulnerability in Apple OS X before 10.11.1 allows local users to bypass intended Gatekeeper restrictions and gain privileges via a Trojan horse program that is loaded from an unexpected directory by an application that has a valid Apple digital signature.

CVE-2015-7024 has been assigned by product-security@apple.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.7 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	HIGH	LOW	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6.9 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
APPLE-SA-2015-10-21-4 OS X El Capitan 10.11.1 and Security Update 2015-007	Vendor Advisory lists.apple.com text/html	APPLE APPLE-SA-2015-10-21-4

About the security content of OS X El Capitan 10.11.1, Security Update 2015-004 Yosemite, and Security Update 2015-007 Mavericks - Apple Support

Vendor Advisory
support.apple.com
text/html

CONFIRM
support.apple.com/HT205375

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→