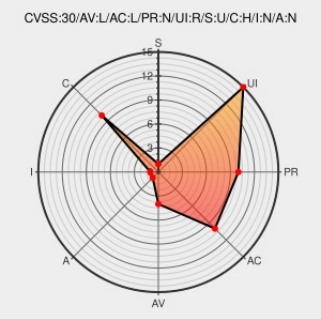
CVE-2017-13782

Published on: 11/12/2017 12:00:00 AM UTC

Last Modified on: 06/12/2023 07:15:00 AM UTC

CVE-2017-13782

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



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

An issue was discovered in certain Apple products. macOS before 10.13.1 is affected. The issue involves the "Kernel" component. It allows attackers to bypass intended memory-read restrictions via a /dev/dtracehelper attack involving the dtrace_dif_variable and dtrace_getarg functions.

CVE-2017-13782 has been assigned by product-security@apple.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.5 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
Using QL to find a memory exposure vulnerability in Apple's macOS XNU kernel (CVE-2017-13782) - Blog - LGTM	Technical Description Third Party Advisory web.archive.org	MISC lgtm.com/blog/apple_xnu_dtrace_CVE-2017-13782

	text/html Inactive Link Not Archived	
Apple XNU Kernel Memory Exposure ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/172827/Apple-XNU-Kernel-Memory-Exposure.html
About the security content of macOS High Sierra 10.13.1, Security Update 2017-001 Sierra, and Security Update 2017-004 El Capitan - Apple Support	Vendor Advisory support.apple.com text/html	CONFIRM support.apple.com/HT208221
Apple macOS Multiple Flaws Let Remote Users Execute Arbitrary Code and Deny Service, Let Local Users Obtain Potentially Sensitive Information, and Applications Gain Elevated Privileges - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	SECTRACK 1039710

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→