



CVE-2014-1372

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

Summary

CVE	CVE-2014-1372
State	PUBLISHED
Assigner	apple
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-07-01 10:17:27 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Graphics Driver in Apple OS X before 10.9.4 does not properly restrict read operations during processing of an unspecified

Risk And Classification

Primary CVSS: v2.0 4.9 from nvd@nist.gov

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

Problem Types: CWE-264 | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

None

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Mac Os X	10.8.0	All	All	All

Operating System	Apple	Mac Os X	10.8.1	All	All	All
Operating System	Apple	Mac Os X	10.8.2	All	All	All
Operating System	Apple	Mac Os X	10.8.3	All	All	All
Operating System	Apple	Mac Os X	10.8.4	All	All	All
Operating System	Apple	Mac Os X	10.8.5	All	All	All
Operating System	Apple	Mac Os X	10.8.5	supplemental_update	All	All
Operating System	Apple	Mac Os X	10.9	All	All	All
Operating System	Apple	Mac Os X	10.9.1	All	All	All
Operating System	Apple	Mac Os X	10.9.2	All	All	All
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
About Secunia Research Flexera
NEOHAPSIS - Peace of Mind Through Integrity and Insight
Issue 18 - google-security-research - OS X IOKit kernel memory disclosure due to lack of bounds checking in AGPMClient::getPstatesOccupa
Apple OS X Bugs Let Remote Users Execute Arbitrary Code and Local Users Gain Elevated Privileges - SecurityTracker
About the security content of OS X Mavericks v10.9.4 and Security Update 2014-003 - Apple Support
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.