



# CVE-2018-4251

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

## Summary

<b>CVE</b>	CVE-2018-4251
<b>State</b>	PUBLIC
<b>Assigner</b>	product-security@apple.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-06-08 18:29:00 UTC
<b>Updated</b>	2019-10-03 00:03:00 UTC
<b>Description</b>	An issue was discovered in certain Apple products. macOS before 10.13.5 is affected. The issue involves the "Firmware" co

## Risk And Classification

**Problem Types:** CWE-732

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	All	All	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	All	All	All	All

## References

### Reference

- Apple macOS/OS X Multiple Flaws Let Remote Users Execute Arbitrary Code and Deny Service and Let Local Users Obtain Potentially Sensitive Information
- Full Disclosure: Repeat of CVE-2018-4251 in Razer Laptops
- About the security content of macOS High Sierra 10.13.5, Security Update 2018-003 Sierra, Security Update 2018-003 El Capitan - 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.

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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)