

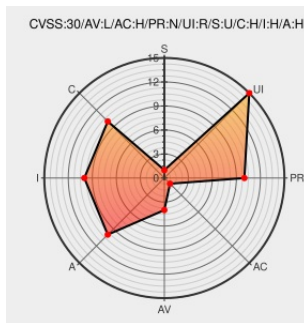


CVE-2018-4230

Published on: 06/08/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:15 PM UTC

CVE-2018-4230

[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 10.13.5 is affected. The issue involves the "NVIDIA Graphics Drivers" component. It allows attackers to execute arbitrary code in a privileged context via a crafted app that triggers a SetAppSupportBits use-after-free because of a race condition.

CVE-2018-4230 has been assigned by product-security@apple.com to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7 - HIGH**

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

CVSS2 Score: **7.6 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	HIGH	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Apple macOS/OS X Multiple Flaws Let Remote Users Execute Arbitrary Code and Deny Service and Let Local Users Obtain Potentially Sensitive Information, Bypass Security, and Gain Elevated Privileges - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com	SECTrack 1041027

[text/html](#)

Apple macOS Kernel - Use-After-Free Due to Lack of Locking in nvidia GeForce Driver - macOS dos Exploit

[Third Party Advisory](#)
[VDB Entry](#)
[www.exploit-db.com](#)
[Proof of Concept](#)
[text/html](#)

 [EXPLOIT-DB 44847](#)

1549 - project-zero - Project Zero - Monorail

[Exploit](#)
[Third Party Advisory](#)
[bugs.chromium.org](#)
[text/html](#)

 [MISC](#)
[bugs.chromium.org/p/project-zero/issues/detail?id=1549](#)

About the security content of macOS High Sierra 10.13.5, Security Update 2018-003 Sierra, Security Update 2018-003 El Capitan - Apple Support

[Vendor Advisory](#)
[support.apple.com](#)
[text/html](#)

 [CONFIRM](#)
[support.apple.com/HT208849](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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	Mac Os X	All	All	All	All
cpe:2.3:o:apple:mac_os_x:*****:*****:						
cpe:2.3:o:apple:mac_os_x:*****:*****:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#).

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