

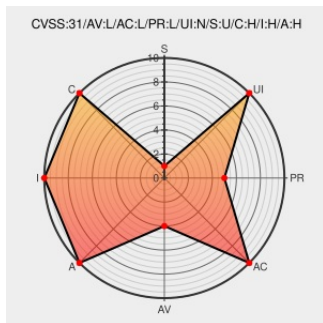


CVE-2015-7892

Published on: 12/09/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:12 PM UTC

CVE-2015-7892

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [M2m1shot Driver](#) from [Samsung](#) contain the following vulnerability:

Stack-based buffer overflow in the m2m1shot_compat_ioctl32 function in the Samsung m2m1shot driver framework, as used in Samsung S6 Edge, allows local users to have unspecified impact via a large data.buf_out.num_planes value in an ioctl call.

CVE-2015-7892 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.8 - HIGH**

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

CVSS2 Score: **4.6 - MEDIUM**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Issue 493 - google-security-research - Samsung m2m1shot kernel driver buffer overflow - Google Security Research - Google Project Hosting	Exploit Third Party Advisory code.google.com text/html	MISC code.google.com/p/google-security-research/issues/detail?id=493

Samsung - 'm2m1shot' Kernel Driver Buffer Overflow - Android
dos Exploit

Exploit

Third Party Advisory

VDB Entry

www.exploit-db.com

Proof of Concept

text/html

MISC www.exploit-db.com/exploits/38555/

Samsung M2m1shot Kernel Driver Buffer Overflow ≈ Packet
Storm

Exploit

Third Party Advisory

VDB Entry

packetstormsecurity.com

text/html

MISC
packetstormsecurity.com/files/134108/Samsung-M2m1shot-Kernel-Driver-Buffer-Overflow.html

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
Application	Samsung	M2m1shot Driver	-	All	All	All
Application	Samsung	M2m1shot Driver	-	All	All	All
cpe:2.3:a:samsung:m2m1shot_driver:-:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:a:samsung:m2m1shot_driver:-:~::~~::~~::~~::~~::~~::~~::						

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](#)