



CVE-2021-31785

Published on: 09/07/2021 12:00:00 AM UTC

Last Modified on: 05/03/2022 04:04:00 PM UTC

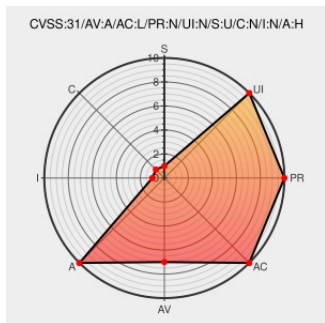
CVE-2021-31785

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Ats2815](#) from [Actions-semi](#) contain the following vulnerability:

The Bluetooth Classic implementation on Actions ATS2815 and ATS2819 chipsets does not properly handle the reception of multiple LMP_host_connection_req packets, allowing attackers in radio range to trigger a denial of service (deadlock) of the device via crafted LMP packets. Manual user intervention is required to restart the device and restore Bluetooth communication.

CVE-2021-31785 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.5 - MEDIUM**

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

CVSS2 Score: **6.1 - MEDIUM**

Access Vector	Access Complexity	Authentication
ADJACENT_NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	COMPLETE

CVE References

Description	Tags	Link
	dl.packetstormsecurity.net application/pdf	MISC dl.packetstormsecurity.net/papers/general/braktooth.pdf

There are currently no QIDs associated with this CVE

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Actions-semi	Ats2815	-	All	All	All
Operating System	Actions-semi	Ats2815 Firmware	-	All	All	All
Hardware	Actions-semi	Ats2819	-	All	All	All
Hardware	Actions-semi	Ats2819p	-	All	All	All
Operating System	Actions-semi	Ats2819p Firmware	-	All	All	All
Hardware	Actions-semi	Ats2819s	-	All	All	All
Operating System	Actions-semi	Ats2819s Firmware	-	All	All	All
Hardware	Actions-semi	Ats2819t	-	All	All	All
Operating System	Actions-semi	Ats2819t Firmware	-	All	All	All
Operating System	Actions-semi	Ats2819 Firmware	-	All	All	All
cpe:2.3:h:actions-semi:ats2815:-:*:*:*:*:*:						
cpe:2.3:o:actions-semi:ats2815_firmware:-:*:*:*:*:*:						
cpe:2.3:h:actions-semi:ats2819:-:*:*:*:*:*:						
cpe:2.3:h:actions-semi:ats2819p:-:*:*:*:*:*:						
cpe:2.3:o:actions-semi:ats2819p_firmware:-:*:*:*:*:*:						
cpe:2.3:h:actions-semi:ats2819s:-:*:*:*:*:*:						
cpe:2.3:o:actions-semi:ats2819s_firmware:-:*:*:*:*:*:						
cpe:2.3:h:actions-semi:ats2819t:-:*:*:*:*:*:						
cpe:2.3:o:actions-semi:ats2819t_firmware:-:*:*:*:*:*:						

```
cpe:2.3:o:actions-semi:ats2819_firmware:-:*:*:*:*:*:
```

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-31785 : The Bluetooth Classic implementation on Actions ATS2815 and ATS2819 chipsets does not properly han... twitter.com/i/web/status/1...	2021-09-07 07:08:59
 @SecRiskRptSME	RT: CVE-2021-31785 The Bluetooth Classic implementation on Actions ATS2815 and ATS2819 chipsets does not properly... twitter.com/i/web/status/1...	2021-09-07 07:33:52

[← 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