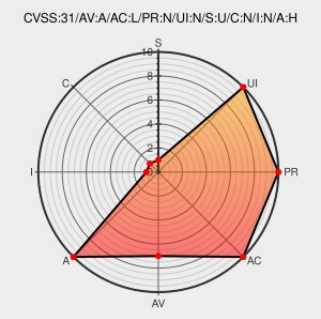
CVE-2021-31787

Published on: 11/30/2021 12:00:00 AM UTC

Last Modified on: 12/03/2021 02:45:00 PM UTC

CVE-2021-31787

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 chipsets does not properly handle the reception of continuous unsolicited LMP responses, allowing attackers in radio range to trigger a denial of service and shutdown of a device by flooding the target device with LMP_features_res packets.

CVE-2021-31787 has been assigned by 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
Launch Studio - Listing Details	launchstudio.bluetooth.com	MISC launchstudio.bluetooth.com/ListingDetails/76427

Launch Studio - Listing Details	launchstudio.bluetooth.com text/html	MISC launchstudio.bluetooth.com/ListingDetails/76427
Bluetooth Speaker _Our ICs_Actions	www.actions-semi.com text/html	MISC www.actions-semi.com/index.php?id=3581&siteId=4

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
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-2021-31787 : The Bluetooth Classic implementation on Actions ATS2815 chipsets does not properly handle the rece… twitter.com/i/web/status/1…	2021-11-30 19:44:14

← Previous ID

Next ID→