



Published on: Not Yet Published

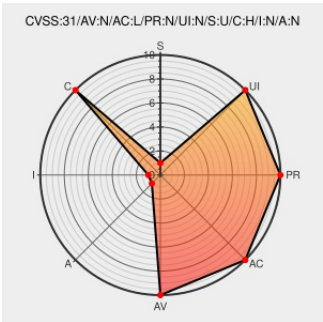
Last Modified on: 02/21/2023 06:00:00 PM UTC

CVE-2022-25738

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF 

Certain versions of [Ar8031](#) from [Qualcomm](#) contain the following vulnerability:

Information disclosure in modem due to buffer over-red while performing checksum of packet received

CVE-2022-25738 has been assigned by  product-security@qualcomm.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
Qualcomm Documentation	www.qualcomm.com text/html	 MISC www.qualcomm.com/company/product-security/bulletins/february-2023-bulletin

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  	Qualcomm	Ar8031	-	All	All	All
Operating System	Qualcomm	Ar8031 Firmware	-	All	All	All
Hardware  	Qualcomm	Csra6620	-	All	All	All
Operating System	Qualcomm	Csra6620 Firmware	-	All	All	All
Hardware  	Qualcomm	Csra6640	-	All	All	All
Operating System	Qualcomm	Csra6640 Firmware	-	All	All	All
Hardware  	Qualcomm	Mdm8207	-	All	All	All
Operating System	Qualcomm	Mdm8207 Firmware	-	All	All	All
Hardware  	Qualcomm	Mdm9205	-	All	All	All
Operating System	Qualcomm	Mdm9205 Firmware	-	All	All	All
Hardware  	Qualcomm	Mdm9206	-	All	All	All
Operating System	Qualcomm	Mdm9206 Firmware	-	All	All	All
Hardware  	Qualcomm	Mdm9207	-	All	All	All
Operating System	Qualcomm	Mdm9207 Firmware	-	All	All	All
Hardware  	Qualcomm	Mdm9607	-	All	All	All
Operating System	Qualcomm	Mdm9607 Firmware	-	All	All	All
Hardware  	Qualcomm	Qca4004	-	All	All	All
Operating System	Qualcomm	Qca4004 Firmware	-	All	All	All
Hardware  	Qualcomm	Qca4010	-	All	All	All
Operating System	Qualcomm	Qca4010 Firmware	-	All	All	All
Hardware  	Qualcomm	Qca4020	-	All	All	All
Operating System	Qualcomm	Qca4020 Firmware	-	All	All	All
Hardware  	Qualcomm	Qca4024	-	All	All	All
Operating System	Qualcomm	Qca4024 Firmware	-	All	All	All
Hardware  	Qualcomm	Qcs405	-	All	All	All
Operating System	Qualcomm	Qcs405 Firmware	-	All	All	All

Hardware  	Qualcomm	Qts110	-	All	All	All
Operating System	Qualcomm	Qts110 Firmware	-	All	All	All
Hardware  	Qualcomm	Ssg2115p	-	All	All	All
Operating System	Qualcomm	Ssg2115p Firmware	-	All	All	All
Hardware  	Qualcomm	Ssg2125p	-	All	All	All
Operating System	Qualcomm	Ssg2125p Firmware	-	All	All	All
Hardware  	Qualcomm	Sxr1230p	-	All	All	All
Operating System	Qualcomm	Sxr1230p Firmware	-	All	All	All
Hardware  	Qualcomm	Sxr2230p	-	All	All	All
Operating System	Qualcomm	Sxr2230p Firmware	-	All	All	All
Hardware  	Qualcomm	Wcd9306	-	All	All	All
Operating System	Qualcomm	Wcd9306 Firmware	-	All	All	All
Hardware  	Qualcomm	Wcd9330	-	All	All	All
Operating System	Qualcomm	Wcd9330 Firmware	-	All	All	All
Hardware  	Qualcomm	Wcd9335	-	All	All	All
Operating System	Qualcomm	Wcd9335 Firmware	-	All	All	All
Hardware  	Qualcomm	Wcd9380	-	All	All	All
Operating System	Qualcomm	Wcd9380 Firmware	-	All	All	All
Hardware  	Qualcomm	Wcd9385	-	All	All	All
Operating System	Qualcomm	Wcd9385 Firmware	-	All	All	All
Hardware  	Qualcomm	Wcn3980	-	All	All	All
Operating System	Qualcomm	Wcn3980 Firmware	-	All	All	All
Hardware  	Qualcomm	Wcn3998	-	All	All	All
Operating System	Qualcomm	Wcn3998 Firmware	-	All	All	All
Hardware  	Qualcomm	Wcn3999	-	All	All	All
Operating System	Qualcomm	Wcn3999 Firmware	-	All	All	All

Hardware		Qualcomm	Wcn6855	-	All	All	All
Operating System		Qualcomm	Wcn6855 Firmware	-	All	All	All
Hardware		Qualcomm	Wcn6856	-	All	All	All
Operating System		Qualcomm	Wcn6856 Firmware	-	All	All	All
Hardware		Qualcomm	Wcn7850	-	All	All	All
Operating System		Qualcomm	Wcn7850 Firmware	-	All	All	All
Hardware		Qualcomm	Wcn7851	-	All	All	All
Operating System		Qualcomm	Wcn7851 Firmware	-	All	All	All
Hardware		Qualcomm	Wsa8810	-	All	All	All
Operating System		Qualcomm	Wsa8810 Firmware	-	All	All	All
Hardware		Qualcomm	Wsa8815	-	All	All	All
Operating System		Qualcomm	Wsa8815 Firmware	-	All	All	All
Hardware		Qualcomm	Wsa8830	-	All	All	All
Operating System		Qualcomm	Wsa8830 Firmware	-	All	All	All
Hardware		Qualcomm	Wsa8832	-	All	All	All
Operating System		Qualcomm	Wsa8832 Firmware	-	All	All	All
Hardware		Qualcomm	Wsa8835	-	All	All	All
Operating System		Qualcomm	Wsa8835 Firmware	-	All	All	All
cpe:2.3:h:qualcomm:ar8031:-:*~::~:							
cpe:2.3:o:qualcomm:ar8031_firmware:-:*~::~:							
cpe:2.3:h:qualcomm:csra6620:-:*~::~:							
cpe:2.3:o:qualcomm:csra6620_firmware:-:*~::~:							
cpe:2.3:h:qualcomm:csra6640:-:*~::~:							
cpe:2.3:o:qualcomm:csra6640_firmware:-:*~::~:							
cpe:2.3:h:qualcomm:mdm8207:-:*~::~:							
cpe:2.3:o:qualcomm:mdm8207_firmware:-:*~::~:							
cpe:2.3:h:qualcomm:mdm9205:-:*~::~:							

```
cpe:2.3:o:qualcomm:mdm9205_firmware:-:*:*:*:*:*:
```

cpe:2.3:h:qualcomm:mdm9206:-:*:*:*:*:*:*:

```
cpe:2.3:o:qualcomm:mdm9206_firmware:-:*:*:*:*:*:
```

cpe:2.3:h:qualcomm:mdm9207:-:*:*:*:*:*:*:

```
cpe:2.3:o:qualcomm:mdm9207_firmware:-:*:*:*:*:*:
```

```
cpe:2.3:h:qualcomm:mdm9607:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:mdm9607_firmware:-:*:*:*:*:*:
```

cpe:2.3:h:qualcomm:qca4004:-:*:*:*:*:*:*:

```
cpe:2.3:o:qualcomm:qca4004_firmware:-:*:*:*:*:*:*:
```

cpe:2.3:h:qualcomm:qca4010:-:*:*:*:*:*:*:

```
cpe:2.3:o:qualcomm:qca4010_firmware:-:*:*:*:*:*:*:
```

cpe:2.3:h:qualcomm:qca4020:-:*:*:*:*:*:*:

```
cpe:2.3:o:qualcomm:qca4020_firmware:-:*:*:*:*:*:*:
```

cpe:2.3:h:qualcomm:qca4024:-:*:*:*:*:*:*:

```
cpe:2.3:o:qualcomm:qca4024_firmware:-:*:*:*:*:*:*:
```

cpe:2.3:h:qualcomm:gcs405:-:*:*:*:*:*:*:

```
cpe:2.3:o:qualcomm:qcs405_firmware:-:*:*:*:*:*:*:
```

cpe:2.3:h:qualcomm:qts110:-:*:*:*:*:*:*:

```
cpe:2.3:o:qualcomm:gts110_firmware:-:*:*:*:*:*:*
```

cpe:2.3:h:qualcomm:ssg2115p:-:*:*:*:*:*:

```
cpe:2.3:o:qualcomm:ssg2115p_firmware:-:*:*:*:*:*:
```

cpe:2.3:h:qualcomm:ssg2125p:-:*:*:*:*:*:

```
cpe:2.3:o:qualcomm:ssg2125p_firmware:-:*:*:*:*:*:*:
```

cpe:2.3:h:qualcomm:sxr1230p:-:*:*:*:*:*:

```
cpe:2.3:o:qualcomm:sxr1230p_firmware:-:*:*:*:*:
```

cpe:2.3:h:qualcomm:sxr2230p:-:*:*:*:*:*:

```
cpe:2.3:o:qualcomm:sxr2230p_firmware:-:*:*:*:*:*:*
```

```
cpe:2.3:h:qualcomm:wcd9306:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:wcd9306 firmware:-:*:*:*:*:*.*
```

cpe:2.3:h:qualcomm:wcd9330:-:*****:
cpe:2.3:o:qualcomm:wcd9330_firmware:-:*****:
cpe:2.3:h:qualcomm:wcd9335:-:*****:
cpe:2.3:o:qualcomm:wcd9335_firmware:-:*****:
cpe:2.3:h:qualcomm:wcd9380:-:*****:
cpe:2.3:o:qualcomm:wcd9380_firmware:-:*****:
cpe:2.3:h:qualcomm:wcd9385:-:*****:
cpe:2.3:o:qualcomm:wcd9385_firmware:-:*****:
cpe:2.3:h:qualcomm:wcn3980:-:*****:
cpe:2.3:o:qualcomm:wcn3980_firmware:-:*****:
cpe:2.3:h:qualcomm:wcn3998:-:*****:
cpe:2.3:o:qualcomm:wcn3998_firmware:-:*****:
cpe:2.3:h:qualcomm:wcn3999:-:*****:
cpe:2.3:o:qualcomm:wcn3999_firmware:-:*****:
cpe:2.3:h:qualcomm:wcn6855:-:*****:
cpe:2.3:o:qualcomm:wcn6855_firmware:-:*****:
cpe:2.3:h:qualcomm:wcn6856:-:*****:
cpe:2.3:o:qualcomm:wcn6856_firmware:-:*****:
cpe:2.3:h:qualcomm:wcn7850:-:*****:
cpe:2.3:o:qualcomm:wcn7850_firmware:-:*****:
cpe:2.3:h:qualcomm:wcn7851:-:*****:
cpe:2.3:o:qualcomm:wcn7851_firmware:-:*****:
cpe:2.3:h:qualcomm:wsa8810:-:*****:
cpe:2.3:o:qualcomm:wsa8810_firmware:-:*****:
cpe:2.3:h:qualcomm:wsa8815:-:*****:
cpe:2.3:o:qualcomm:wsa8815_firmware:-:*****:
cpe:2.3:h:qualcomm:wsa8830:-:*****:
cpe:2.3:o:qualcomm:wsa8830_firmware:-:*****:

```
cpe:2.3:h:qualcomm:wsa8832:-:*:*:*:*:*:
cpe:2.3:o:qualcomm:wsa8832_firmware:-:*:*:*:*:*:
cpe:2.3:h:qualcomm:wsa8835:-:*:*:*:*:*:
cpe:2.3:o:qualcomm:wsa8835_firmware:-:*:*:*:*:*:
```

```
cpe:2.3:h:qualcomm:wsa8832:-:*:*:*:*:*:
cpe:2.3:o:qualcomm:wsa8832_firmware:-:*:*:*:*:*:
cpe:2.3:h:qualcomm:wsa8835:-:*:*:*:*:*:
cpe:2.3:o:qualcomm:wsa8835_firmware:-:*:*:*:*:*:
```

```
cpe:2.3:h:qualcomm:wsa8832:-:*:*:*:*:*:
cpe:2.3:o:qualcomm:wsa8832_firmware:-:*:*:*:*:*:
cpe:2.3:h:qualcomm:wsa8835:-:*:*:*:*:*:
cpe:2.3:o:qualcomm:wsa8835_firmware:-:*:*:*:*:*:
```

```
cpe:2.3:h:qualcomm:wsa8832:-:*:*:*:*:*:
cpe:2.3:o:qualcomm:wsa8832_firmware:-:*:*:*:*:*:
cpe:2.3:h:qualcomm:wsa8835:-:*:*:*:*:*:
cpe:2.3:o:qualcomm:wsa8835_firmware:-:*:*:*:*:*:
```

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-25738 : Information disclosure in modem due to buffer over-red while performing checksum of packet receive... twitter.com/i/web/status/1...	2023-02-12 04:07:50
 @JohnJasonFallow	New vulnerability on the NVD: CVE-2022-25738 ift.tt/AJD1vrX	2023-02-12 06:11:07
 @doogsineerg	New vulnerability on the NVD: CVE-2022-25738 ift.tt/SUqnBpM	2023-02-12 06:33:25
 @xanadulinux	CVE-2022-25738 ift.tt/I9BP5zv	2023-02-12 06:52:24
 /r/netcve	CVE-2022-25738	2023-02-12 04:38:17

[← 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