



# CVE-2021-31505

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2021-31505
<b>State</b>	PUBLIC
<b>Assigner</b>	zdi-disclosures@trendmicro.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-06-29 15:15:00 UTC
<b>Updated</b>	2021-07-07 17:42:00 UTC
<b>Description</b>	This vulnerability allows attackers with physical access to escalate privileges on affected installations of Arlo Q Plus 1.9.0.3

## Risk And Classification

**Problem Types:** CWE-798

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	<a href="#">Arlo</a>	<a href="#">Q Plus</a>	-	All	All	All
Operating System	<a href="#">Arlo</a>	<a href="#">Q Plus Firmware</a>	1.9.0.3_278	All	All	All

## References

Reference	Source	Link
ZDI-21-683   Zero Day Initiative	MISC	<a href="http://www.zerodayinitiative.com">www.zerodayinitiative.com</a>
Security Advisory for Arlo Q Plus SSH Use of Hard-coded Credentials Allowing Privilege Escalation	MISC	<a href="http://kb.arlo.com">kb.arlo.com</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)