



CVE-2018-16525

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

Summary

CVE	CVE-2018-16525
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-12-06 23:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	Amazon Web Services (AWS) FreeRTOS through 1.3.1, FreeRTOS up to V10.0.1 (with FreeRTOS+TCP), and WITTENST

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Amazon	Amazon Web Services Freertos	All	All	All	All
Application	Amazon	Freertos	All	All	All	All

References

Reference

- [amazon-freertos/CHANGELOG.md at v1.3.2 · aws/amazon-freertos · GitHub](#)
- [FreeRTOS TCP/IP Stack Vulnerabilities Put A Wide Range of Devices at Risk of Compromise: From Smart Homes to Critical Infrastructure Systems](#)
- [FreeRTOS TCP/IP Stack Vulnerabilities - The Details | Zimperium Mobile Security Blog](#)
- [CVE Program record](#)
- [NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[11646](#) Amazon Web Services (AWS) FreeRTOS Buffer Overflow Vulnerability

© [CVE.report](#) 2026 |

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](#)