



CVE-2018-16417

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

Summary

CVE	CVE-2018-16417
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-10-30 17:15:00 UTC
Updated	2020-08-24 17:37:00 UTC
Description	Aruba Instant 4.x prior to 6.4.4.8-4.2.4.12, 6.5.x prior to 6.5.4.11, 8.3.x prior to 8.3.0.6, and 8.4.x prior to 8.4.0.1 allows Cor

Risk And Classification

Problem Types: CWE-77

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Arubanetworks	Instant	All	All	All	All
Operating System	Arubanetworks	Instant	All	All	All	All
Hardware	Siemens	W1750d	-	All	All	All
Hardware	Siemens	W1750d	-	All	All	All
Operating System	Siemens	W1750d Firmware	All	All	All	All
Operating System	Siemens	W1750d Firmware	All	All	All	All

References

Reference
CVE-2018-16417 CVE-2018-7064 CVE-2018-7084 CVE-2018-7083 CVE-2018-7082 Siemens SCALANCE W1750D ICESA-19-134-07 Multiple
www.arubanetworks.com/assets/alert/ARUBA-PSA-2019-001.txt
cert-portal.siemens.com/productcert/pdf/ssa-549547.pdf
Malformed Request
Siemens SCALANCE W1750D CISA
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

© [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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)