



CVE-2021-25657

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

Summary

CVE	CVE-2021-25657
State	PUBLIC
Assigner	securityalerts@avaya.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-09-02 01:15:00 UTC
Updated	2022-09-07 19:48:00 UTC
Description	A privilege escalation vulnerability was discovered in Avaya IP Office Admin Lite and USB Creator that may potentially allow

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Avaya	Ip Office	All	All	All	All
Application	Avaya	Ip Office	11.1	-	All	All
Application	Avaya	Ip Office	11.1	feature_pack1	All	All
Application	Avaya	Ip Office	11.1	feature_pack1_service_pack1	All	All
Application	Avaya	Ip Office	11.1	feature_pack2	All	All
Application	Avaya	Ip Office	11.1	feature_pack2_service_pack1	All	All

References

Reference	Source	Link	T
Vulnerability-Disclosures/MNDR-2022-0037.md at master · mandiant/Vulnerability-Disclosures · GitHub	MISC	github.com	
ASA-2022-114	CONFIRM	support.avaya.com	
CVE Program record	CVE.ORG	www.cve.org	c
NVD vulnerability detail	NVD	nvd.nist.gov	c

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](#).

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