



CVE-2022-26481

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

Summary

CVE	CVE-2022-26481
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-07-17 23:15:00 UTC
Updated	2022-07-21 22:46:00 UTC
Description	An issue was discovered in Poly Studio before 3.7.0. Command Injection can occur via the CN field of a Create Certificate S

Risk And Classification

Problem Types: CWE-78

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Poly	G7500	-	All	All	All
Operating System	Poly	G7500 Firmware	All	All	All	All
Hardware	Poly	Studio X30	-	All	All	All
Operating System	Poly	Studio X30 Firmware	All	All	All	All
Hardware	Poly	Studio X50	-	All	All	All
Operating System	Poly	Studio X50 Firmware	All	All	All	All
Hardware	Poly	Studio X70	-	All	All	All
Operating System	Poly	Studio X70 Firmware	All	All	All	All

References

Reference	Source	Link	Tags
Security Center Poly, formerly Plantronics & Polycom	MISC	www.poly.com	
Authenticated Command Injection in Poly Studio	MISC	sec-consult.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

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](#)