



CVE-2015-8300

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2015-8300
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-08-28 21:29:00 UTC
Updated	2018-09-26 21:29:00 UTC
Description	Polycom BToE Connector before 3.0.0 uses weak permissions (Everyone: Full Control) for "Program Files (x86)\polycom\p

Risk And Classification

Problem Types: CWE-275

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Polycom	Btoe Connector	All	All	All	All

References

Reference	Source	Link
Full Disclosure: CVE-2015-8300: Polycom BToE Connector v2.3.0 Privilege Escalation Vulnerability	FULLDISC	seclists.org
advisories/2015/Polycom_20150513 at public · sbaresearch/advisories · GitHub	MISC	github.com
Polycom BTOE Connector 2.3.0 Local Privilege Escalation ≈ Packet Storm	MISC	packetstormsecurity.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](#).

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