CVE-2020-7036

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-7036
State	PUBLIC
Assigner	securityalerts@avaya.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-04-23 21:15:00 UTC
Updated	2021-04-30 16:51:00 UTC
Description	An XML External Entities (XXE)vulnerability in Callback Assist could allow an authenticated, remote attacker to gain read ac

Risk And Classification

Problem Types: CWE-611

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Avaya	Callback Assist	All	All	All	All
Application	Avaya	Callback Assist	4.7.1.1	-	All	All
Application	Avaya	Callback Assist	4.7.1.1	patch1	All	All
Application	Avaya	Callback Assist	4.7.1.1	patch2	All	All
Application	Avaya	Callback Assist	4.7.1.1	patch3	All	All
Application	Avaya	Callback Assist	4.7.1.1	patch4	All	All
Application	Avaya	Callback Assist	4.7.1.1	patch5	All	All
Application	Avaya	Callback Assist	4.7.1.1	patch6	All	All

References

Reference	Source	Link	Tags
ASA-2021-030	CONFIRM	downloads.avaya.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 and Source URL Uptime Status status.cve.report