CVE-2020-7032

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-7032
State	PUBLIC
Assigner	securityalerts@avaya.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-11-13 01:15:00 UTC
Updated	2022-10-19 14:39:00 UTC
Description	An XML external entity (XXE) vulnerability in Avaya WebLM admin interface allows authenticated users to read arbitrary file

Risk And Classification

Problem Types: CWE-611

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Avaya	Aura System Manager	All	All	All	All
Application	Avaya	Aura System Manager	All	All	All	All
Application	Avaya	Weblm	All	All	All	All
Application	Avaya	Weblm	All	All	All	All
Application	Avaya	Weblm	All	All	All	All

References

Reference	Source
Avaya Web License Manager XML Injection ≈ Packet Storm	MISC
ASA-2020-153	CONFIRM
Full Disclosure: SEC Consult SA-20201117-0 :: Blind Out-Of-Band XML External Entity Injection in Avaya Web License Manager	FULLDISC
Blind Out-of-band XML External Entity Injection In Avaya Web License Manager	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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