



# CVE-2019-4513

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2019-4513
<b>State</b>	PUBLIC
<b>Assigner</b>	psirt@us.ibm.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-08-26 15:15:00 UTC
<b>Updated</b>	2022-12-02 22:25:00 UTC
<b>Description</b>	IBM Security Access Manager for Enterprise Single Sign-On 8.2.2 is vulnerable to an XML External Entity Injection (XXE) a

## Risk And Classification

**Problem Types:** CWE-611

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	ibm	Security Access Manager For Enterprise Single Sign-on	8.2.2	All	All	All
Application	ibm	Security Access Manager For Enterprise Single Sign-on	8.2.2	All	All	All

## References

### Reference

Security Bulletin: IBM Security Access Manager for Enterprise Single-Sign On is affected by an XML External Entity Injection (XXE) vulnerabili

IBM X-Force Exchange

CVE Program record

NVD vulnerability detail

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](#)**