



# CVE-2020-7329

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

## Summary

<b>CVE</b>	CVE-2020-7329
<b>State</b>	PUBLIC
<b>Assigner</b>	psirt@mcafee.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-11-11 10:15:00 UTC
<b>Updated</b>	2023-11-16 14:23:00 UTC
<b>Description</b>	Server-side request forgery vulnerability in the ePO extension in McAfee MVISION Endpoint prior to 20.11 allows remote at

## Risk And Classification

**Problem Types:** CWE-918

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Mcafee</a>	<a href="#">Mvision Endpoint</a>	All	All	All	All
Application	<a href="#">Mcafee</a>	<a href="#">Mvision Endpoint</a>	All	All	All	All

## References

### Reference

McAfee Security Bulletin - MVISION Endpoint ePO Extension 20.11 update fixes two vulnerabilities (CVE-2020-7328 and CVE-2020-7329)

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.

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](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)