



# CVE-2019-1490

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

## Summary

<b>CVE</b>	CVE-2019-1490
<b>State</b>	PUBLIC
<b>Assigner</b>	secure@microsoft.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-12-10 22:15:00 UTC
<b>Updated</b>	2020-08-24 17:37:00 UTC
<b>Description</b>	A spoofing vulnerability exists when a Skype for Business Server does not properly sanitize a specially crafted request, aka

## Risk And Classification

**Problem Types:** CWE-74

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Skype For Business	2019	cumulative_update_2	All	All
Application	Microsoft	Skype For Business	2019	cumulative_update_2	All	All

## References

Reference	Source	Link	Tags
portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1490	MISC	<a href="https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1490">portal.msrc.microsoft.com</a>	Patch, Vendor Advis
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

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](#).

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