# CVE-2020-3430

MITRE | NVD | CVE.ORG | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2020-3430 |
| **State** | PUBLIC |
| **Assigner** | psirt@cisco.com |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2020-09-04 03:15:00 UTC |
| **Updated** | 2023-11-07 03:22:00 UTC |
| **Description** | A vulnerability in the application protocol handling features of Cisco Jabber for Windows could allow an unauthenticated, re |

## Risk And Classification

**Problem Types:** CWE-78

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Cisco | Jabber | All | All | All | All |
| Application | Cisco | Jabber | All | All | All | All |

## References

| Reference | Source | Link | Tags |
|---|---|---|---|
| Cisco Jabber for Windows Protocol Handler Command Injection Vulnerability | CISCO | tools.cisco.com | Vendor Advisory |
| 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**