# CVE-2020-7033

MITRE | NVD | CVE.ORG | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2020-7033 |
| **State** | PUBLIC |
| **Assigner** | securityalerts@avaya.com |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2020-11-13 00:15:00 UTC |
| **Updated** | 2020-11-29 21:32:00 UTC |
| **Description** | A Cross Site Scripting (XSS) Vulnerability on the Unified Portal Client (web client) used in Avaya Equinox Conferencing car |

## Risk And Classification

**Problem Types:** CWE-79

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Avaya | Equinox Conferencing | All | All | All | All |
| Application | Avaya | Equinox Conferencing | All | All | All | All |

## References

| Reference | Source | Link | Tags |
|---|---|---|---|
| ASA-2020-152 | CONFIRM | downloads.avaya.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**