



# CVE-2020-35725

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

## Summary

<b>CVE</b>	CVE-2020-35725
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-01-11 03:15:00 UTC
<b>Updated</b>	2023-11-07 03:22:00 UTC
<b>Description</b>	** UNSUPPORTED WHEN ASSIGNED ** Reflected XSS in Quest Policy Authority 8.1.2.200 allows remote attackers to inj

## Risk And Classification

**Problem Types:** CWE-79

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Quest</a>	<a href="#">Policy Authority For Unified Communications</a>	8.1.2.200	All	All	All
Application	<a href="#">Quest</a>	<a href="#">Policy Authority For Unified Communications</a>	8.1.2.200	All	All	All

## References

Reference	Source	Link
Advisory: Multiple Vulnerabilities in Quest Policy Authority for Unified Communications — Un4gi	MISC	<a href="https://un4gi.io">un4gi.io</a>
Advisory: Quest Policy Authority for Unified Communications - Multiple Vulnerabilities — Clandestine Labs	MISC	<a href="https://clandestinelabs.io">clandestinelabs.io</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

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](https://status.cve.report)**