



# CVE-2020-27010

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2020-27010   |
| <b>State</b>           | PUBLIC   |
| <b>Assigner</b>        | security@trendmicro.com  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback   |
| <b>Published</b>       | 2020-12-17 21:15:00 UTC  |
| <b>Updated</b>         | 2020-12-21 21:33:00 UTC  |
| <b>Description</b>     | A cross-site scripting (XSS) vulnerability in Trend Micro InterScan Web Security Virtual Appliance 6.5 SP2 could allow an at |

## Risk And Classification

### Problem Types: CWE-79

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor     | Product                                  | Version | Update | Edition | Language |
|-------------|------------|--|---------|--------|---------|----------|
| Application | Trendmicro | Interscan Web Security Virtual Appliance | 6.5     | sp2    | All     | All      |
| Application | Trendmicro | Interscan Web Security Virtual Appliance | 6.5     | sp2    | All     | All      |

## References

| Reference   | Source |
|---|--------|
| SECURITY BULLETIN: December 2020 Security Bulletin for Trend Micro InterScan Web Security Virtual Appliance (IWSVA) 6.5 SP2 | N/A    |
| CVE Program record  | CVE    |
| NVD vulnerability detail  | NVD    |

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)