



CVE-2020-27013

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

Summary

| | |
|------------------------|----------------------------------------------------------------------------------------------------------------------------|
| CVE | CVE-2020-27013 |
| State | PUBLIC |
| Assigner | security@trendmicro.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2020-10-14 15:15:00 UTC |
| Updated | 2020-10-26 16:35:00 UTC |
| Description | Trend Micro Antivirus for Mac 2020 (Consumer) contains a vulnerability in the product that occurs when a webserver is star |

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|----------------------------|---------------------------|---------|--------|---------|----------|
| Application | Trendmicro | Antivirus | 2020 | All | All | All |
| Application | Trendmicro | Antivirus | 2020 | All | All | All |

References

| Reference | Source |
|--------------------------------------------------------------------------------------------------------------------------------------|--------|
| ZDI-20-1243 Zero Day Initiative | N/A |
| Security Bulletin: Trend Micro Antivirus for Mac Improper Access Control Information Disclosure Vulnerability · Trend Micro for Home | N/A |
| CVE Program record | CVE.C |
| NVD vulnerability detail | NVD |

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](#)