



CVE-2020-28575

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

Summary

CVE	CVE-2020-28575
State	PUBLIC
Assigner	security@trendmicro.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-12-01 19:15:00 UTC
Updated	2020-12-02 15:46:00 UTC
Description	A heap-based buffer overflow privilege escalation vulnerability in Trend Micro ServerProtect for Linux 3.0 may allow an atta

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Trendmicro	Serverprotect	3.0	All	All	All
Application	Trendmicro	Serverprotect	3.0	All	All	All

References

Reference	Source	Link	Tags
New KHM for heap-based buffer overflow privilege - ServerProtect for Linux	MISC	success.trendmicro.com	Vendor Advisory
ZDI-20-1378 Zero Day Initiative	MISC	www.zerodayinitiative.com	Third Party 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.

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](#)