



CVE-2017-11398

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2017-11398
State	PUBLIC
Assigner	security@trendmicro.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-01-19 19:29:00 UTC
Updated	2019-10-09 23:22:00 UTC
Description	A session hijacking via log disclosure vulnerability in Trend Micro Smart Protection Server (Standalone) versions 3.2 and be

Risk And Classification

Problem Types: CWE-534

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Trendmicro	Smart Protection Server	All	All	All	All

References

Reference

- Trend Micro Smart Protection Server Multiple Security Vulnerabilities
- SECURITY BULLETIN: Trend Micro Smart Protection Server (Standalone) Multiple Vulnerabilities
- Trend Micro Smart Protection Server Multiple Vulnerabilities | Core Security
- Trend Micro Smart Protection Server - Session Hijacking / Log File Disclosure / Remote Command Execution / Cron Job Injection / Local File
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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](#)