CVE-2017-5565

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2017-5565
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-03-21 16:59:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	Code injection vulnerability in Trend Micro Maximum Security 11.0 (and earlier), Internet Security 11.0 (and earlier), and An

Risk And Classification

Problem Types: CWE-427

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Trendmicro	Antivirus	All	All	All	All
Application	Trendmicro	Antivirus	All	All	All	All
Application	Trendmicro	Internet Security	All	All	All	All
Application	Trendmicro	Maximum Security	All	All	All	All
Application	Trendmicro	Premium Security	All	All	All	All

References

Reference
DoubleAgent: Zero-Day Code Injection and Persistence Technique | Vulnerabilities Detection
Multiple Trend Micro Products CVE-2017-5565 DLL Loading Local Code Injection Vulnerability
Apply Hot Fix Build 1403 to resolve CVE-2017-5565
Trend Micro Internet Security Application Verifier Provider DLL Protection Flaw Lets Local Users Bypass Anti-Virus Protections and Gain Eleva
DoubleAgent: Taking Full Control Over Your Antivirus | Vulnerabilities Detection
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.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**