CVE-2014-3922

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

Summary

CVE	CVE-2014-3922
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-05-30 14:55:00 UTC
Updated	2016-09-06 13:21:00 UTC
Description	Cross-site scripting (XSS) vulnerability in Trend Micro InterScan Messaging Security Virtual Appliance 8.5.1.1516 allows re

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Trendmicro	Interscan Messaging Security Virtual Appliance	8.5.1.1516	All	All	All
Application	Trendmicro	Interscan Messaging Security Virtual Appliance	8.5.1.1516	All	All	All

References

Reference
Security Advisory SA58491 - Trend Micro InterScan Messaging Security Virtual Appliance "addWhiteListDomainStr" Cross-Site Sc
Trend Micro InterScan Messaging Security Virtual Appliance Input Validation Hole Permits Cross-Site Scripting Attacks - SecurityTracker
Trend Micro InterScan Messaging Security Virtual Appliance Cross Site Scripting Vulnerability
Full Disclosure: XSS Attacks vulnerability in InterScan Messaging Security Virtual Appliance 8.5.1.1516 (Zero-DAY)
Cookie Theft/Session Hijacking IMSVA on Vimeo
InterScan Messaging Security Virtual Appliance 8.5.1.1516 Cross Site Scripting ≈ Packet Storm
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