



CVE-2017-9812

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

Summary

CVE	CVE-2017-9812
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-07-17 21:29:00 UTC
Updated	2017-08-12 01:29:00 UTC
Description	The reportId parameter of the getReportStatus action method can be abused in the web interface in Kaspersky Anti-Virus fr

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Kaspersky	Anti-virus For Linux Server	All	All	All	All

References

Reference
Kaspersky Anti-Virus File Server 8.0.3.297 - Multiple Vulnerabilities - Linux webapps Exploit
Full Disclosure: [CORE-2017-0003] - Kaspersky Anti-Virus File Server Multiple Vulnerabilities
Kaspersky Anti-Virus for Linux File Server Multiple Security Vulnerabilities
Kaspersky Anti-Virus File Server Multiple Vulnerabilities Core Security
Kaspersky Anti-Virus for Linux File Server Multiple Flaws Let Remote Users Conduct Cross-Site Scripting and Cross-Site Request Forgery Att
Kaspersky Anti-Virus File Server 8.0.3.297 XSS / CSRF / Code Execution ≈ 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.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)