



CVE-2017-5607

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

Summary

CVE	CVE-2017-5607
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-04-10 15:59:00 UTC
Updated	2019-03-20 19:23:00 UTC
Description	Splunk Enterprise 5.0.x before 5.0.18, 6.0.x before 6.0.14, 6.1.x before 6.1.13, 6.2.x before 6.2.13.1, 6.3.x before 6.3.10, 6.

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Splunk	Splunk	All	All	All	All
Application	Splunk	Splunk	All	All	All	All
Application	Splunk	Splunk	All	All	All	All

References

Reference
Splunk Bugs Let Remote Users Obtain Potentially Sensitive Information and Remote Authenticated Users Conduct Cross-Site Scripting Attack
hyp3rlinx.altervista.org/advisories/SPLUNK-ENTERPRISE-INFORMATION-THEFT.txt
Splunk Enterprise 6.5.3, 6.2.13.1 and Splunk Light 6.5.2 address multiple vulnerabilities Splunk
Splunk Enterprise CVE-2017-5607 Information Disclosure Vulnerability
Splunk Enterprise - Information Disclosure
Full Disclosure: Splunk Enterprise Information Theft - CVE-2017-5607
Splunk Enterprise HTML Injection Vulnerability
SecurityFocus
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](#)