



CVE-2015-7604

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

Summary

CVE	CVE-2015-7604
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-09-29 19:59:13 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Cross-site scripting (XSS) vulnerability in Splunk Web in Splunk Enterprise 6.2.x before 6.2.6 and Splunk Light 6.2.x before

Risk And Classification

Primary CVSS: v2.0 4.3 from nvd@nist.gov

AV:N/AC:M/Au:N/C:N/I:P/A:N

Problem Types: CWE-79 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

AV:N/AC:M/Au:N/C:N/I:P/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Splunk	Splunk	6.2.0	All	All	All

Application	Splunk	Splunk	6.2.0	All	All	All
Application	Splunk	Splunk	6.2.1	All	All	All
Application	Splunk	Splunk	6.2.1	All	All	All
Application	Splunk	Splunk	6.2.2	All	All	All
Application	Splunk	Splunk	6.2.2	All	All	All
Application	Splunk	Splunk	6.2.3	All	All	All
Application	Splunk	Splunk	6.2.3	All	All	All
Application	Splunk	Splunk	6.2.4	All	All	All
Application	Splunk	Splunk	6.2.4	All	All	All
Application	Splunk	Splunk	6.2.5	All	All	All
Application	Splunk	Splunk	6.2.5	All	All	All

Vendor Declared Affected Products					
Source	Vendor	Product	Version	Platforms	
CNA	Na	N/a	affected n/a	Not specified	

References	
Reference	Source
Splunk Input Validation Flaw in Splunk Web Lets Remote Conduct Cross-Site Scripting Attacks - SecurityTracker	af854a3a-2127-422b-91a6
Splunk Enterprise 6.2.6 and Splunk Light 6.2.6 address one vulnerability Splunk	af854a3a-2127-422b-91a6
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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