



CVE-2017-8768

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

Summary

CVE	CVE-2017-8768
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-05-04 22:29:00 UTC
Updated	2017-05-17 16:04:00 UTC
Description	Atlassian SourceTree v2.5c and prior are affected by a command injection in the handling of the sourcetree:// scheme. It wi

Risk And Classification

Problem Types: CWE-78

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Atlassian	Sourcetree	All	All	All	All

References

Reference	Source	Link	Tags
oss-security - Sourcetree arbitrary command execution	MISC	openwall.com	Mailing List, Third Party Adv
Full Disclosure: [oss-security]Sourcetree arbitrary command execution	MISC	seclists.org	Mailing List, Third Party Adv
sourcetree arbitrary command execution. - YouTube	MISC	www.youtube.com	Third Party Advisory
Atlassian SourceTree CVE-2017-8768 Command Injection Vulnerability	BID	www.securityfocus.com	Third Party Advisory, VDB E
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

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