



CVE-2018-20236

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

Summary

CVE	CVE-2018-20236
State	PUBLIC
Assigner	security@atlassian.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-03-08 18:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	There was an command injection vulnerability in Sourcetree for Windows from version 0.5a before version 3.0.10 via URI h

Risk And Classification

Problem Types: CWE-77

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference
Sourcetree Git Arbitrary Code Execution / URL Handling ≈ Packet Storm
[SRCTREEWIN-11291] Command Injection via URI handling in Sourcetree for Windows - CVE-2018-20236 - Create and track feature request
Malformed Request
Bugtraq: March 2019 Sourcetree Advisory - Multiple Remote Code Execution Vulnerabilities
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](#)