



CVE-2020-36233

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

Summary

CVE	CVE-2020-36233
State	PUBLIC
Assigner	security@atlassian.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-02-18 20:15:00 UTC
Updated	2021-02-24 19:30:00 UTC
Description	The Microsoft Windows Installer for Atlassian Bitbucket Server and Data Center before version 6.10.9, 7.x before 7.6.4, and

Risk And Classification

Problem Types: CWE-276

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Atlassian	Bitbucket	All	All	All	All
Application	Atlassian	Bitbucket	All	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All

References

Reference

VU#240785 - Atlassian Bitbucket on Windows is vulnerable to privilege escalation due to weak ACLs
[BSERV-12753] Privilege Escalation Vulnerability in Atlassian Bitbucket on Windows - CVE-2020-36233 - Create and track feature requests for
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[730309](#) Atlassian Bitbucket Privilege Escalation Vulnerability (CVE-2020-36233)

© [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](#).

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