



CVE-2019-7238

Published on: 03/21/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:53 PM UTC

CVE-2019-7238

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Nexus](#) from [Sonatype](#) contain the following vulnerability:

Sonatype Nexus Repository Manager before 3.15.0 has Incorrect Access Control.

CVE-2019-7238 has been assigned by [M](#) [cve@mitre.org](#) to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **7.5 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
CVE-2019-7238 Nexus Repository Manager 3 - Missing Access Controls and Remote Code Execution - 2019-02-05 – Sonatype Support	Vendor Advisory support.sonatype.com text/html	MISC support.sonatype.com/hc/en-us/articles/360017310793-CVE-2019-7238-Nexus-Repository-Manager-3-Missing-Access-Controls-and-Remote-Code-Execution-February-5th-2019

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Exploit/POC from Github

Nexus Repository Manager 3 Remote Code Execution without authentication < 3.15.0

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sonatype	Nexus	All	All	All	All
Application	Sonatype	Nexus	All	All	All	All
cpe:2.3:a:sonatype:nexus:*****:						
cpe:2.3:a:sonatype:nexus:*****:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @cipherstorm	Update to CVE-2019-7238 in Nexus Repository Manager 3: Today, an article was brought to our attention that suggests... twitter.com/i/web/status/1...	2021-04-12 14:25:36
 @security_inside	Update to CVE-2019-7238 in Nexus Repository Manager 3 securityboulevard.com/2021/04/update...	2021-04-12 14:30:36
 @IT_securitynews	Update to CVE-2019-7238 in Nexus Repository Manager 3 itsecuritynews.info/update-to-cve-...	2021-04-12 15:03:55
 @netsecu	securityboulevard.com/2021/04/update... 403 Forbidden #cybersecurity	2021-04-12 15:31:05
 @malware_devil	Update to #cve-2019-7238 in Nexus #repository Manager 3 malwaredevil.com/2021/04/12/upd... #attack #cve #repository... twitter.com/i/web/status/1...	2021-04-12 19:11:27
 @thenewstack	Update to CVE-2019-7238 in Nexus Repository Manager 3 bit.ly/3tdGiTU @sonatype	2021-04-14 05:47:00
 @pwnwikiorg	CVE-2019-7238 Nexus Repository Manger extdirect 遠程命令執行漏洞 pwnwiki.org/index.php?titl...	2021-07-08 06:27:23
 @sec715	[CVE-2019-7238] NEXUS < 3.14.0 Remote Code Execution. #bugbountytips #rce #nexus https://t.co/P50NxdV1I	2021-08-12 12:40:21
 @TheMsterDoctor1	[CVE-2019-7238] NEXUS < 3.14.0 Remote Code Execution. #bugbountytips #rce #nexus https://t.co/8KMWvLiGMY	2021-08-12 12:43:24
 @ipssignatures	The vuln CVE-2019-7238 has a tweet created 0 days ago and retweeted 11 times. twitter.com/sec715/status/... #pow1rtrwwcve	2021-08-12 15:06:00

© [CVE.report](#) 2023  |

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](#)