



CVE-2019-12395

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

Summary

CVE	CVE-2019-12395
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-05-28 13:29:00 UTC
Updated	2021-11-08 19:47:00 UTC
Description	In Webbukit Dynmap 3.0-beta-3 or below, due to a missing login check in servlet/MapStorageHandler.java, an attacker can

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Dynmap Project	Dynmap	All	All	All	All
Application	Dynmap Project	Dynmap	3.0	alpha1	All	All
Application	Dynmap Project	Dynmap	3.0	alpha2	All	All
Application	Dynmap Project	Dynmap	3.0	alpha3	All	All
Application	Dynmap Project	Dynmap	3.0	beta3	All	All
Application	Dynmap Project	Dynmap	3.0	rc3	All	All
Application	Dynmap Project	Dynmap	3.0	beta3	All	All
Application	Getbukkit	Spigot	1.13.2	All	All	All
Application	Getbukkit	Spigot	1.13.2	All	All	All

References

Reference	Source	Link	Tags
Required login bypass vulnerability · Issue #2474 · webbukit/dynmap · GitHub	MISC	github.com	Exploit, Tr
Fix required login bypass vulnerability by Ry0taK · Pull Request #2475 · webbukit/dynmap · GitHub	MISC	github.com	Patch, Thi
Merge pull request #2475 from Ry0taK/v3.0 · webbukit/dynmap@641f142 · GitHub	MISC	github.com	Patch, Thi
JVN#89046645: A map plugin for Minecraft server "Dynmap" fails to restrict access permissions	JVN	jvn.jp	
CVE Program record	CVE.ORG	www.cve.org	canonical

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://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](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). 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