



CVE-2018-10682

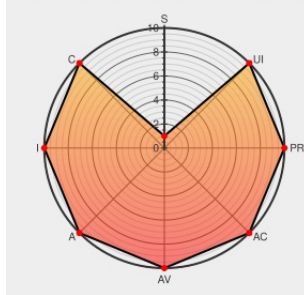
Published on: 05/09/2018 12:00:00 AM UTC

Last Modified on: 11/07/2023 02:51:00 AM UTC

CVE-2018-10682

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

CVSS:30/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



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

**** DISPUTED **** An issue was discovered in WildFly 10.1.2.Final. It is possible for an attacker to access the administration panel on TCP port 9990 without any authentication using "anonymous" access that is automatically created. Once logged in, a misconfiguration present by default (auto-deployment) permits an anonymous user to deploy a malicious .war file, leading to remote code execution. NOTE: the vendor indicates that anonymous access is not available in the default installation; however, it remains optional because there are several use cases for it, including development environments and network architectures that have a proxy server for access control to the WildFly server.

CVE-2018-10682 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: **10 - HIGH**

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

CVE References

Description	Tags	Link				
exploit/CVE-2018-10682-CVE-2018-10683.txt at master · kmkz/exploit · GitHub	Exploit Third Party Advisory github.com text/html	 MISC github.com/kmkz/exploit/blob/master/CVE-2018-10682-CVE-2018-10683.txt				
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						
Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Wildfly	Wildfly	10.1.2	final	All	All
Application	Wildfly	Wildfly	10.1.2	final	All	All
cpe:2.3:a:wildfly:wildfly:10.1.2:final:****.*.*:						
cpe:2.3:a:wildfly:wildfly:10.1.2:final:****.*.*:						
No vendor comments have been submitted for this CVE						
← Previous ID			Next ID →			