



CVE-2020-26515

Published on: 06/08/2021 12:00:00 AM UTC

Last Modified on: 10/18/2023 07:04:00 PM UTC

CVE-2020-26515

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

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

An insufficiently protected credentials issue was discovered in Intland codeBeamer ALM 10.x through 10.1.SP4. The remember-me cookie (CB_LOGIN) issued by the application contains the encrypted user's credentials. However, due to a bug in the application code, those credentials are encrypted using a NULL encryption key.

CVE-2020-26515 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

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

CVSS2 Score: **5 - MEDIUM**

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

CVE References

Description	Tags	Link
	www.compass-security.com text/x-c	MISC www.compass-security.com/fileadmin/Research/Advisories/2021-09_CSNC-2020-010-codebeamer_ALM_Insecure-RememberMe.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

Exploit/POC from Github

PoC for exploiting CVE-2020-26515 : An insufficiently protected credentials issue was discovered in Intland codeBeame...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Intland	Codebeamer	All	All	All	All
Application	Intland	Codebeamer	10.1.0	-	All	All
Application	Intland	Codebeamer	10.1.0	sp1	All	All
Application	Intland	Codebeamer	10.1.0	sp2	All	All
Application	Intland	Codebeamer	10.1.0	sp3	All	All
Application	Intland	Codebeamer	10.1.0	sp4	All	All
Application	Intland	Codebeamer Application Lifecycle Management	All	All	All	All
Application	Intland	Codebeamer Application Lifecycle Management	10.1.0	-	All	All
Application	Intland	Codebeamer Application Lifecycle Management	10.1.0	sp1	All	All
Application	Intland	Codebeamer Application Lifecycle Management	10.1.0	sp2	All	All
Application	Intland	Codebeamer Application Lifecycle Management	10.1.0	sp3	All	All
Application	Intland	Codebeamer Application Lifecycle Management	10.1.0	sp4	All	All

cpe:2.3:a:intland:codebeamer:*****:.*:

cpe:2.3:a:intland:codebeamer:10.1.0:-:.*:.*:.*:.*:

cpe:2.3:a:intland:codebeamer:10.1.0:sp1:*****:.*:

cpe:2.3:a:intland:codebeamer:10.1.0:sp2:*****:.*:

cpe:2.3:a:intland:codebeamer:10.1.0:sp3:*****:.*:

cpe:2.3:a:intland:codebeamer:10.1.0:sp4:*****:.*:

cpe:2.3:a:intland:codebeamer_application_lifecycle_management:*****:.*:

cpe:2.3:a:intland:codebeamer_application_lifecycle_management:10.1.0:-:.*:.*:.*:.*:

cpe:2.3:a:intland:codebeamer_application_lifecycle_management:10.1.0:sp1:*****:		
cpe:2.3:a:intland:codebeamer_application_lifecycle_management:10.1.0:sp2:*****:		
cpe:2.3:a:intland:codebeamer_application_lifecycle_management:10.1.0:sp3:*****:		
cpe:2.3:a:intland:codebeamer_application_lifecycle_management:10.1.0:sp4:*****:		
No vendor comments have been submitted for this CVE		
Social Mentions		
Source	Title	Posted (UTC)
 @CVereport	CVE-2020-26515 : An insufficiently protected credentials issue was discovered in Intland codeBeamer ALM 10.x through... twitter.com/i/web/status/1...	2021-06-08 13:04:58
 /r/netcve	CVE-2020-26515	2021-06-08 13:41:18
← Previous ID		Next ID →

© [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](#)