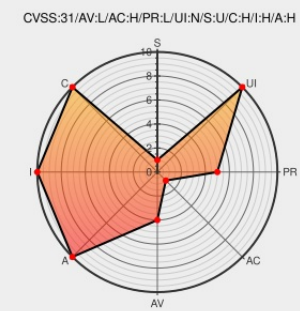
CVE-2022-3182

Published on: Not Yet Published

Last Modified on: 09/20/2022 07:09:00 PM UTC

CVE-2022-3182

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Remote Desktop Manager from Devolutions contain the following vulnerability:

Improper Access Control vulnerability in the Duo SMS two-factor of Devolutions Remote Desktop Manager 2022.2.14 and earlier allows attackers to bypass the application lock. This issue affects: Devolutions Remote Desktop Manager version 2022.2.14 and prior versions.

CVE-2022-3182 has been assigned by security@devolutions.net to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Devolutions** - **Remote Desktop Manager** version **<= 2022.2.14**

CVSS3 Score: 7 - HIGH

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

CVE References

Description	Tags	Link
DEVO-2022-0007 - Devolutions	devolutions.net text/html	MISC devolutions.net/security/advisories/DEVO-2022-0007

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Devolutions	Remote Desktop Manager	All	All	All	All

cpe:2.3:a:devolutions:remote_desktop_manager:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-3182 : Improper Access Control vulnerability in the Duo SMS two-factor of Devolutions Remote Desktop Manag… twitter.com/i/web/status/1…	2022-09-13 20:03:13
/r/netcve	CVE-2022-3182	2022-09-13 20:38:28

← Previous ID

Next ID→