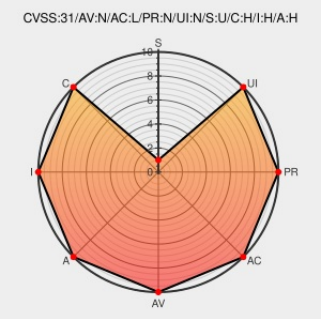
CVE-2020-15487

Published on: 09/30/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:40 PM UTC

CVE-2020-15487

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



Certain versions of Re from Re-desk contain the following vulnerability:

Re:Desk 2.3 contains a blind unauthenticated SQL injection vulnerability in the getBaseCriteria() function in the protected/models/Ticket.php file. By modifying the folder GET parameter, it is possible to execute arbitrary SQL statements via a crafted URL. Unauthenticated remote command execution is possible by using this SQL injection to update certain database values, which are then executed by a bizRule eval() function in the yii/framework/web/auth/CAuthManager.php file. Resultant authorization bypass is also possible, by recovering or modifying password hashes and password reset tokens, allowing for administrative privileges to be obtained.

CVE-2020-15487 has been assigned by 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
Re:Desk v2.3 - Multiple Issues	Exploit Third Party Advisory labs.f-secure.com text/html	MISC labs.f-secure.com/advisories/redesk-v2-3-multiple-issues/
Download Help Desk Ticketing Software Open Source	Vendor Advisory www.re-desk.com text/html	MISC www.re-desk.com/download-help-desk-software.html

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Re-desk	Re	desk	2.3	All	All
Application	Re-desk	Re	desk	2.3	All	All

cpe:2.3:a:re-desk:re\:desk:2.3:*:*:*:*:*:*:*

cpe:2.3:a:re-desk:re\:desk:2.3:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→