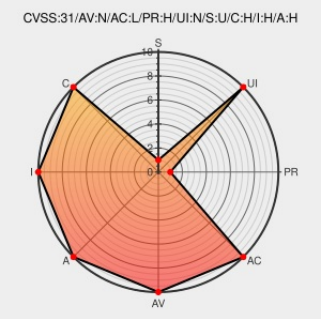
CVE-2020-15849

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

Last Modified on: 03/23/2021 11:23:41 PM UTC

CVE-2020-15849

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



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

Re:Desk 2.3 has a blind authenticated SQL injection vulnerability in the SettingsController class, in the actionEmailTemplates() method. A malicious actor with access to an administrative account could abuse this vulnerability to recover sensitive data from the application's database, allowing for authorization bypass and taking over additional accounts by means of modifying password-reset tokens stored in the database. Remote command execution is also possible by leveraging this to abuse the Yii framework's bizRule functionality, allowing for arbitrary PHP code to be executed by the application. Remote command execution is also possible by using this together with a separate insecure file upload vulnerability (CVE-2020-15488).

CVE-2020-15849 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.2 - HIGH

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

CVSS2 Score: 6.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
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	Product 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→