



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](#)

CVSS:31/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H



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 [M](#) 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

Re:Desk v2.3 - Multiple Issues

Tags

Exploit

Third Party Advisory

labs.f-secure.com

text/html

Link

 MISC labs.f-secure.com/advisories/redesk-v2-3-multiple-issues/

Description

Download Help Desk Ticketing Software Open Source

Tags

Product

Vendor Advisory

www.re-desk.com

text/html

Link

 MISC www.re-desk.com/download-help-desk-software.html

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	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 →