



CVE-2021-20796

Published on: 10/13/2021 12:00:00 AM UTC

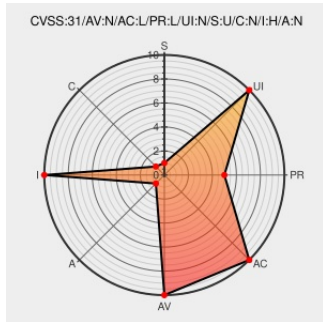
Last Modified on: 10/19/2021 07:05:00 PM UTC

CVE-2021-20796

Source: Mitre

Source: Nist

Print: PDF



Certain versions of [Remote Service Manager](#) from [Cybozu](#) contain the following vulnerability:

Directory traversal vulnerability in the management screen of Cybozu Remote Service 3.1.8 allows a remote authenticated attacker to upload an arbitrary file via unspecified vectors.

CVE-2021-20796 has been assigned by [vultures@jpcert.or.jp](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [Cybozu, Inc.](#) - **Cybozu Remote Service** version **3.1.8**

CVSS3 Score: **6.5 - MEDIUM**

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

CVSS2 Score: **4 - MEDIUM**

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

CVE References

Description	Tags	Link
不具合情報公開サイト	kb.cybozu.support/text/html	MISC kb.cybozu.support/article/37427

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	Cybozu	Remote Service Manager	3.1.8	All	All	All
cpe:2.3:a:cybozu:remote_service_manager:3.1.8:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @management_sun	IT Risk:サイボウズ リモートサービスにおける複数の脆弱性 -2/3 サイボウズ リモートサービス 3.1.8:CVE-2021-20796、CVE-2021-20797、CVE-2021-20800 サイボウズ リモートサ... twitter.com/i/web/status/1...	2021-09-30 04:01:25
 @management_sun	IT Risk:Multiple vulnerabilities in Cybozu remote services -2/3 Cybozu Remote Service 3.1.8:CVE-2021-20796、CVE-2021... twitter.com/i/web/status/1...	2021-09-30 04:02:54
 @CVEreport	CVE-2021-20796 : Directory traversal vulnerability in the management screen of Cybozu Remote Service 3.1.8 allows a... twitter.com/i/web/status/1...	2021-10-13 08:36:55

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2021   |

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](#)