

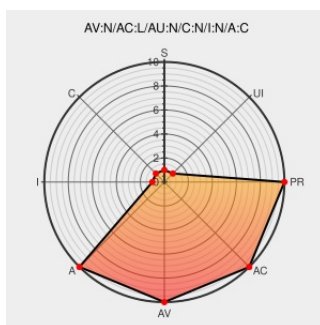


CVE-2014-7266

Published on: 02/01/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:50 PM UTC

CVE-2014-7266

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

Algorithmic complexity vulnerability in Cybozu Remote Service Manager through 2.3.0 and 3.x through 3.1.2 allows remote attackers to cause a denial of service (CPU consumption) via vectors that trigger colliding hash-table keys. NOTE: this vulnerability exists because of an incomplete fix for CVE-2014-1983.

CVE-2014-7266 has been assigned by [vultures@jpcert.or.jp](#) to track the vulnerability

CVSS2 Score: **7.8 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

NONE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

JVN#13566542: Cybozu Remote Service Manager vulnerable to denial-of-service (DoS)

[Vendor Advisory](#)

[JVN JVN#13566542](#)

[jvn.jp](#)

[text/xml](#)

No Description Provided

[Vendor Advisory](#)

[JVND JVND-2015-000001](#)

[jvndb.jvn.jp](#)

[text/html](#)

【サイボウズ リモートサービス】脆弱性対応について | サイボウズからのお知らせ

[Patch](#)

[CONFIRM](#)

[Vendor Advisory](#)

[cs.cybozu.co.jp/2015/001245.html](#)

[cs.cybozu.co.jp](#)

[text/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	Cybozu	Remote Service Manager	2.3.0	All	All	All
Application	Cybozu	Remote Service Manager	3.1.0	All	All	All
Application	Cybozu	Remote Service Manager	3.1.1	All	All	All
Application	Cybozu	Remote Service Manager	3.1.2	All	All	All
Application	Cybozu	Remote Service Manager	2.3.0	All	All	All
Application	Cybozu	Remote Service Manager	3.1.0	All	All	All
Application	Cybozu	Remote Service Manager	3.1.1	All	All	All
Application	Cybozu	Remote Service Manager	3.1.2	All	All	All
cpe:2.3:a:cybozu:remote_service_manager:2.3.0:*****:.*						
cpe:2.3:a:cybozu:remote_service_manager:3.1.0:*****:.*						
cpe:2.3:a:cybozu:remote_service_manager:3.1.1:*****:.*						
cpe:2.3:a:cybozu:remote_service_manager:3.1.2:*****:.*						
cpe:2.3:a:cybozu:remote_service_manager:2.3.0:*****:.*						
cpe:2.3:a:cybozu:remote_service_manager:3.1.0:*****:.*						
cpe:2.3:a:cybozu:remote_service_manager:3.1.1:*****:.*						
cpe:2.3:a:cybozu:remote_service_manager:3.1.2:*****:.*						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)