



CVE-2013-6003

Published on: 12/05/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:37 PM UTC

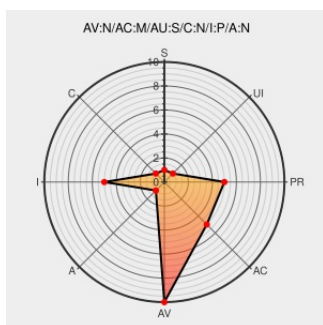
CVE-2013-6003

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Garoon](#) from [Cybozu](#) contain the following vulnerability:

CRLF injection vulnerability in Cybozu Garoon 3.1 through 3.5 SP5, when Phone Messages forwarding is enabled, allows remote authenticated users to inject arbitrary e-mail headers via unspecified vectors.

CVE-2013-6003 has been assigned by vultures@jpcert.or.jp to track the vulnerability

CVSS2 Score: **3.5 - LOW**

Access
Vector

Access
Complexity

Authentication

NETWORK

MEDIUM

SINGLE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

NONE

PARTIAL

NONE

CVE References

Description

Tags

Link

サイボウズ ガルーン 3.7 脆弱性情報のお知らせ【CY13-12-001】 | サイボウズからのお知らせ

cs.cybozu.co.jp
text/html

MISC
cs.cybozu.co.jp/information/20131202up01.php

No Description Provided

jvndb.jvn.jp
text/html

JVND JB VJND-2013-000116

JVN#84221103: Cybozu Garoon vulnerable to mail header injection

jvn.jp
text/xml

JVN JVN#84221103

不具合情報公開サイト

Vendor Advisory
support.cybozu.com
text/html

CONFIRM support.cybozu.com/ja-jp/article/6121

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

CVS Report does not endorse any commercial products that may be mentioned in these check. Read additional 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	Garoon	3.1	All	All	All
Application	Cybozu	Garoon	3.1	sp1	All	All
Application	Cybozu	Garoon	3.1	sp2	All	All
Application	Cybozu	Garoon	3.1	sp3	All	All
Application	Cybozu	Garoon	3.5	All	All	All
Application	Cybozu	Garoon	3.5	sp1	All	All
Application	Cybozu	Garoon	3.5	sp2	All	All
Application	Cybozu	Garoon	3.5	sp3	All	All
Application	Cybozu	Garoon	3.5	sp4	All	All
Application	Cybozu	Garoon	3.5	sp5	All	All
Application	Cybozu	Garoon	3.1	All	All	All
Application	Cybozu	Garoon	3.1	sp1	All	All
Application	Cybozu	Garoon	3.1	sp2	All	All
Application	Cybozu	Garoon	3.1	sp3	All	All
Application	Cybozu	Garoon	3.5	All	All	All
Application	Cybozu	Garoon	3.5	sp1	All	All
Application	Cybozu	Garoon	3.5	sp2	All	All
Application	Cybozu	Garoon	3.5	sp3	All	All
Application	Cybozu	Garoon	3.5	sp4	All	All
Application	Cybozu	Garoon	3.5	sp5	All	All

cpe:2.3:a:cybozu:garoon:3.1:*:*:*:*:*:*:

cpe:2.3:a:cybozu:garoon:3.1:sp1:*:*:*:*:*:

cpe:2.3:a:cybozu:garoon:3.1:sp2:*:*:*:*:*:

cpe:2.3:a:cybozu:garoon:3.1:sp3:*:*:*:*:

```
cpe:2.3:a:cybozu:garoon:3.5:*:*:*:*:*:*:
```

cpe:2.3:a:cybozu:garoon:3.5:sp1:.*:.*:.*:.*:.*:.*

cpe:2.3:a:cybozu:garoon:3.5:sp2:*:*:*:*:*:

cpe:2.3:a:cybozu:garoon:3.5:sp3:*:*:*:*:*:

cpe:2.3:a:cybozu:garoon:3.5:sp4:*****:
cpe:2.3:a:cybozu:garoon:3.5:sp5:*****:
cpe:2.3:a:cybozu:garoon:3.1:*****:
cpe:2.3:a:cybozu:garoon:3.1:sp1:*****:
cpe:2.3:a:cybozu:garoon:3.1:sp2:*****:
cpe:2.3:a:cybozu:garoon:3.1:sp3:*****:
cpe:2.3:a:cybozu:garoon:3.5:*****:
cpe:2.3:a:cybozu:garoon:3.5:sp1:*****:
cpe:2.3:a:cybozu:garoon:3.5:sp2:*****:
cpe:2.3:a:cybozu:garoon:3.5:sp3:*****:
cpe:2.3:a:cybozu:garoon:3.5:sp4:*****:
cpe:2.3:a:cybozu:garoon:3.5:sp5:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)