Certain versions of Php Rrd Web Client from Ganglia contain the following vulnerability:

graph.php in Ganglia PHP RRD Web Client 1.0.2 allows remote attackers to execute arbitrary commands via the command parameter, which is provided to the passthru function.

CVE-2002-2104 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.5 - HIGH

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

CVE References


IBM X-Force Exchange

Ganglia PHP RRD Web Client Remote Command Execution Vulnerability

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)

<table>
<thead>
<tr>
<th>Type</th>
<th>Vendor</th>
<th>Product</th>
<th>Version</th>
<th>Update</th>
<th>Edition</th>
<th>Language</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Ganglia</td>
<td>Php Rrd Web Client</td>
<td>1.0.1</td>
<td>All</td>
<td>All</td>
<td>All</td>
</tr>
<tr>
<td>Application</td>
<td>Ganglia</td>
<td>Php Rrd Web Client</td>
<td>1.0.1</td>
<td>All</td>
<td>All</td>
<td>All</td>
</tr>
</tbody>
</table>

```
cpe:2.3:a:ganglia:php_rrd_web_client:1.0.1:*:*:*:*:*:*:  
cpe:2.3:a:ganglia:php_rrd_web_client:1.0.1:*:*:*:*:*:*:  
```

No vendor comments have been submitted for this CVE

© CVE.report 2022

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