CVE-2012-2104

Published on: 08/26/2012 12:00:00 AM UTC
Last Modified on: 03/23/2021 11:28:26 PM UTC

Certain versions of Munin from Munin-monitoring contain the following vulnerability:

cgi-bin/munin-cgi-graph in Munin 2.x writes data to a log file without sanitizing non-printable characters, which might allow user-assisted remote attackers to inject terminal emulator escape sequences and execute arbitrary commands or delete arbitrary files via a crafted HTTP request.

CVE-2012-2104 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 6.8 - MEDIUM

Access Vector | Access Complexity | Authentication
--------------|-------------------|-----------------
NETWORK       | MEDIUM            | NONE

Confidentiality Impact | Integrity Impact | Availability Impact
PARTIAL          | PARTIAL           | PARTIAL

CVE References

Description | Tags | Link
-------------|------|------
#668666 - munin-cgi-graph: enables injecting arbitrary strings into munin-cgi-graph.log - Debian Bug report logs | bugs.debian.org | MISC bugs.debian.org/cgi-bin/bugreport.cgi?bug=668666
Citrix SD-WAN Multiple Security Updates | support.citrix.com | CONFIRM support.citrix.com/article/CTX236992
Munin Remote Command Injection Vulnerability | Exploit | BID 53032
IBM X-Force Exchange | exchange.xforce.ibmcloud.com | XF munin-munincgigraphlog-command-execution(74885)
oss-security - CVE Request (minor) -- Two Munin graphing framework flaws | www.openwall.com | MLIST [oss-security] 20120416 CVE Request (minor) -- Two Munin graphing framework flaws
framework flaws

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>Munin-monitoring</td>
<td>Munin</td>
<td>2.0</td>
<td>All</td>
<td>All</td>
<td>All</td>
</tr>
<tr>
<td>Application</td>
<td>Munin-monitoring</td>
<td>Munin</td>
<td>2.1</td>
<td>All</td>
<td>All</td>
<td>All</td>
</tr>
<tr>
<td>Application</td>
<td>Munin-monitoring</td>
<td>Munin</td>
<td>2.0</td>
<td>All</td>
<td>All</td>
<td>All</td>
</tr>
<tr>
<td>Application</td>
<td>Munin-monitoring</td>
<td>Munin</td>
<td>2.1</td>
<td>All</td>
<td>All</td>
<td>All</td>
</tr>
</tbody>
</table>

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