



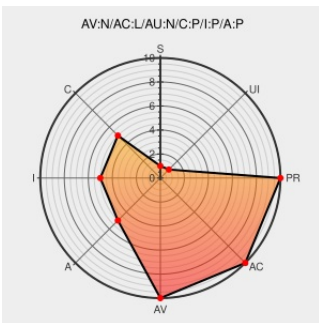
Last Modified on: 03/23/2021 11:28:17 PM UTC

CVE-2012-3374

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF 

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

Buffer overflow in markup.c in the MXit protocol plugin in libpurple in Pidgin before 2.10.5 allows remote attackers to execute arbitrary code via a crafted inline image in a message.

CVE-2012-3374 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
Pidgin Security Advisories	Vendor Advisory web.archive.org text/html Inactive Link Not Archived	 CONFIRM www.pidgin.im/news/security/index.php?id=64
Support / Security / Advisories // MDVSA-2012:105 Mandriva	www.mandriva.com text/html	 MANDRIVA MDVSA-2012:105
[security-announce] SUSE-SU-2012:0890-1: important: Security update for	lists.opensuse.org text/html	 SUSE SUSE-SU-2012:0890
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2012:1102
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval:org.mitre.oval:def:17678

Security Advisory SA50005 - Red Hat update for pidgin - Secunia

[web.archive.org](#)
[text/html](#)

SECUNIA 50005

pidgin/main: changeset ded93865ef42

[Exploit](#)
[Patch](#)
[hg.pidgin.im](#)
[text/xml](#)

CONFIRM
[hg.pidgin.im/pidgin/main/rev/ded93865ef42](#)

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	Pidgin	Pidgin	2.0.0	All	All	All
Application	Pidgin	Pidgin	2.0.1	All	All	All
Application	Pidgin	Pidgin	2.0.2	All	All	All
Application	Pidgin	Pidgin	2.1.0	All	All	All
Application	Pidgin	Pidgin	2.1.1	All	All	All
Application	Pidgin	Pidgin	2.10.0	All	All	All
Application	Pidgin	Pidgin	2.10.1	All	All	All
Application	Pidgin	Pidgin	2.10.2	All	All	All
Application	Pidgin	Pidgin	2.10.3	All	All	All
Application	Pidgin	Pidgin	2.2.0	All	All	All
Application	Pidgin	Pidgin	2.2.1	All	All	All
Application	Pidgin	Pidgin	2.2.2	All	All	All
Application	Pidgin	Pidgin	2.3.0	All	All	All
Application	Pidgin	Pidgin	2.3.1	All	All	All
Application	Pidgin	Pidgin	2.4.0	All	All	All
Application	Pidgin	Pidgin	2.4.1	All	All	All
Application	Pidgin	Pidgin	2.4.2	All	All	All
Application	Pidgin	Pidgin	2.4.3	All	All	All
Application	Pidgin	Pidgin	2.5.0	All	All	All
Application	Pidgin	Pidgin	2.5.1	All	All	All
Application	Pidgin	Pidgin	2.5.2	All	All	All
Application	Pidgin	Pidgin	2.5.3	All	All	All
Application	Pidgin	Pidgin	2.5.4	All	All	All

Application	Pidgin	Pidgin	2.5.5	All	All	All
Application	Pidgin	Pidgin	2.5.6	All	All	All
Application	Pidgin	Pidgin	2.5.7	All	All	All
Application	Pidgin	Pidgin	2.5.8	All	All	All
Application	Pidgin	Pidgin	2.5.9	All	All	All
Application	Pidgin	Pidgin	2.6.0	All	All	All
Application	Pidgin	Pidgin	2.6.1	All	All	All
Application	Pidgin	Pidgin	2.6.2	All	All	All
Application	Pidgin	Pidgin	2.6.4	All	All	All
Application	Pidgin	Pidgin	2.6.5	All	All	All
Application	Pidgin	Pidgin	2.6.6	All	All	All
Application	Pidgin	Pidgin	2.7.0	All	All	All
Application	Pidgin	Pidgin	2.7.1	All	All	All
Application	Pidgin	Pidgin	2.7.10	All	All	All
Application	Pidgin	Pidgin	2.7.11	All	All	All
Application	Pidgin	Pidgin	2.7.2	All	All	All
Application	Pidgin	Pidgin	2.7.3	All	All	All
Application	Pidgin	Pidgin	2.7.4	All	All	All
Application	Pidgin	Pidgin	2.7.5	All	All	All
Application	Pidgin	Pidgin	2.7.6	All	All	All
Application	Pidgin	Pidgin	2.7.7	All	All	All
Application	Pidgin	Pidgin	2.7.8	All	All	All
Application	Pidgin	Pidgin	2.7.9	All	All	All
Application	Pidgin	Pidgin	2.8.0	All	All	All
Application	Pidgin	Pidgin	2.9.0	All	All	All
Application	Pidgin	Pidgin	2.0.0	All	All	All
Application	Pidgin	Pidgin	2.0.1	All	All	All
Application	Pidgin	Pidgin	2.0.2	All	All	All
Application	Pidgin	Pidgin	2.1.0	All	All	All
Application	Pidgin	Pidgin	2.1.1	All	All	All
Application	Pidgin	Pidgin	2.10.0	All	All	All
Application	Pidgin	Pidgin	2.10.1	All	All	All
Application	Pidgin	Pidgin	2.10.2	All	All	All
Application	Pidgin	Pidgin	2.10.3	All	All	All
Application	Pidgin	Pidgin	2.2.0	All	All	All
Application	Pidgin	Pidgin	2.2.1	All	All	All

Application	Pidgin	Pidgin	2.2.1	All	All	All
Application	Pidgin	Pidgin	2.2.2	All	All	All
Application	Pidgin	Pidgin	2.3.0	All	All	All
Application	Pidgin	Pidgin	2.3.1	All	All	All
Application	Pidgin	Pidgin	2.4.0	All	All	All
Application	Pidgin	Pidgin	2.4.1	All	All	All
Application	Pidgin	Pidgin	2.4.2	All	All	All
Application	Pidgin	Pidgin	2.4.3	All	All	All
Application	Pidgin	Pidgin	2.5.0	All	All	All
Application	Pidgin	Pidgin	2.5.1	All	All	All
Application	Pidgin	Pidgin	2.5.2	All	All	All
Application	Pidgin	Pidgin	2.5.3	All	All	All
Application	Pidgin	Pidgin	2.5.4	All	All	All
Application	Pidgin	Pidgin	2.5.5	All	All	All
Application	Pidgin	Pidgin	2.5.6	All	All	All
Application	Pidgin	Pidgin	2.5.7	All	All	All
Application	Pidgin	Pidgin	2.5.8	All	All	All
Application	Pidgin	Pidgin	2.5.9	All	All	All
Application	Pidgin	Pidgin	2.6.0	All	All	All
Application	Pidgin	Pidgin	2.6.1	All	All	All
Application	Pidgin	Pidgin	2.6.2	All	All	All
Application	Pidgin	Pidgin	2.6.4	All	All	All
Application	Pidgin	Pidgin	2.6.5	All	All	All
Application	Pidgin	Pidgin	2.6.6	All	All	All
Application	Pidgin	Pidgin	2.7.0	All	All	All
Application	Pidgin	Pidgin	2.7.1	All	All	All
Application	Pidgin	Pidgin	2.7.10	All	All	All
Application	Pidgin	Pidgin	2.7.11	All	All	All
Application	Pidgin	Pidgin	2.7.2	All	All	All
Application	Pidgin	Pidgin	2.7.3	All	All	All
Application	Pidgin	Pidgin	2.7.4	All	All	All
Application	Pidgin	Pidgin	2.7.5	All	All	All
Application	Pidgin	Pidgin	2.7.6	All	All	All
Application	Pidgin	Pidgin	2.7.7	All	All	All
Application	Pidgin	Pidgin	2.7.8	All	All	All
Application	Pidgin	Pidgin	2.7.9	All	All	All

Application	Pidgin	Pidgin	2.8.0	All	All	All
Application	Pidgin	Pidgin	2.9.0	All	All	All
Application	Pidgin	Pidgin	All	All	All	All
cpe:2.3:a:pidgin:pidgin:2.0.0:*:*:*:*:*:						
cpe:2.3:a:pidgin:pidgin:2.0.1:*:*:*:*:*:						
cpe:2.3:a:pidgin:pidgin:2.0.2:*:*:*:*:*:						
cpe:2.3:a:pidgin:pidgin:2.1.0:*:*:*:*:*:						
cpe:2.3:a:pidgin:pidgin:2.1.1:*:*:*:*:*:						
cpe:2.3:a:pidgin:pidgin:2.10.0:*:*:*:*:*:						
cpe:2.3:a:pidgin:pidgin:2.10.1:*:*:*:*:*:						
cpe:2.3:a:pidgin:pidgin:2.10.2:*:*:*:*:*:						
cpe:2.3:a:pidgin:pidgin:2.10.3:*:*:*:*:*:						
cpe:2.3:a:pidgin:pidgin:2.2.0:*:*:*:*:*:						
cpe:2.3:a:pidgin:pidgin:2.2.1:*:*:*:*:*:						
cpe:2.3:a:pidgin:pidgin:2.2.2:*:*:*:*:*:						
cpe:2.3:a:pidgin:pidgin:2.3.0:*:*:*:*:*:						
cpe:2.3:a:pidgin:pidgin:2.3.1:*:*:*:*:*:						
cpe:2.3:a:pidgin:pidgin:2.4.0:*:*:*:*:*:						
cpe:2.3:a:pidgin:pidgin:2.4.1:*:*:*:*:*:						
cpe:2.3:a:pidgin:pidgin:2.4.2:*:*:*:*:*:						
cpe:2.3:a:pidgin:pidgin:2.4.3:*:*:*:*:*:						
cpe:2.3:a:pidgin:pidgin:2.5.0:*:*:*:*:*:						
cpe:2.3:a:pidgin:pidgin:2.5.1:*:*:*:*:*:						
cpe:2.3:a:pidgin:pidgin:2.5.2:*:*:*:*:*:						
cpe:2.3:a:pidgin:pidgin:2.5.3:*:*:*:*:*:						
cpe:2.3:a:pidgin:pidgin:2.5.4:*:*:*:*:*:						
cpe:2.3:a:pidgin:pidgin:2.5.5:*:*:*:*:*:						
cpe:2.3:a:pidgin:pidgin:2.5.6:*:*:*:*:*:						
cpe:2.3:a:pidgin:pidgin:2.5.7:*:*:*:*:*:						

cpe:2.3:a:pidgin:pidgin:2.5.8:****:
cpe:2.3:a:pidgin:pidgin:2.5.9:****:
cpe:2.3:a:pidgin:pidgin:2.6.0:****:
cpe:2.3:a:pidgin:pidgin:2.6.1:****:
cpe:2.3:a:pidgin:pidgin:2.6.2:****:
cpe:2.3:a:pidgin:pidgin:2.6.4:****:
cpe:2.3:a:pidgin:pidgin:2.6.5:****:
cpe:2.3:a:pidgin:pidgin:2.6.6:****:
cpe:2.3:a:pidgin:pidgin:2.7.0:****:
cpe:2.3:a:pidgin:pidgin:2.7.1:****:
cpe:2.3:a:pidgin:pidgin:2.7.10:****:
cpe:2.3:a:pidgin:pidgin:2.7.11:****:
cpe:2.3:a:pidgin:pidgin:2.7.2:****:
cpe:2.3:a:pidgin:pidgin:2.7.3:****:
cpe:2.3:a:pidgin:pidgin:2.7.4:****:
cpe:2.3:a:pidgin:pidgin:2.7.5:****:
cpe:2.3:a:pidgin:pidgin:2.7.6:****:
cpe:2.3:a:pidgin:pidgin:2.7.7:****:
cpe:2.3:a:pidgin:pidgin:2.7.8:****:
cpe:2.3:a:pidgin:pidgin:2.7.9:****:
cpe:2.3:a:pidgin:pidgin:2.8.0:****:
cpe:2.3:a:pidgin:pidgin:2.9.0:****:
cpe:2.3:a:pidgin:pidgin:2.0.0:****:
cpe:2.3:a:pidgin:pidgin:2.0.1:****:
cpe:2.3:a:pidgin:pidgin:2.0.2:****:
cpe:2.3:a:pidgin:pidgin:2.1.0:****:
cpe:2.3:a:pidgin:pidgin:2.1.1:****:
cpe:2.3:a:pidgin:pidgin:2.10.0:****:

cpe:2.3:a:pidgin:pidgin:2.10.1:*****:
cpe:2.3:a:pidgin:pidgin:2.10.2:*****:
cpe:2.3:a:pidgin:pidgin:2.10.3:*****:
cpe:2.3:a:pidgin:pidgin:2.2.0:*****:
cpe:2.3:a:pidgin:pidgin:2.2.1:*****:
cpe:2.3:a:pidgin:pidgin:2.2.2:*****:
cpe:2.3:a:pidgin:pidgin:2.3.0:*****:
cpe:2.3:a:pidgin:pidgin:2.3.1:*****:
cpe:2.3:a:pidgin:pidgin:2.4.0:*****:
cpe:2.3:a:pidgin:pidgin:2.4.1:*****:
cpe:2.3:a:pidgin:pidgin:2.4.2:*****:
cpe:2.3:a:pidgin:pidgin:2.4.3:*****:
cpe:2.3:a:pidgin:pidgin:2.5.0:*****:
cpe:2.3:a:pidgin:pidgin:2.5.1:*****:
cpe:2.3:a:pidgin:pidgin:2.5.2:*****:
cpe:2.3:a:pidgin:pidgin:2.5.3:*****:
cpe:2.3:a:pidgin:pidgin:2.5.4:*****:
cpe:2.3:a:pidgin:pidgin:2.5.5:*****:
cpe:2.3:a:pidgin:pidgin:2.5.6:*****:
cpe:2.3:a:pidgin:pidgin:2.5.7:*****:
cpe:2.3:a:pidgin:pidgin:2.5.8:*****:
cpe:2.3:a:pidgin:pidgin:2.5.9:*****:
cpe:2.3:a:pidgin:pidgin:2.6.0:*****:
cpe:2.3:a:pidgin:pidgin:2.6.1:*****:
cpe:2.3:a:pidgin:pidgin:2.6.2:*****:
cpe:2.3:a:pidgin:pidgin:2.6.4:*****:
cpe:2.3:a:pidgin:pidgin:2.6.5:*****:
cpe:2.3:a:pidgin:pidgin:2.6.6:*****:
cpe:2.3:a:pidgin:pidgin:2.7.0:*****:

cpe:2.3:a:pidgin:pidgin:2.7.1:****:*:*:
cpe:2.3:a:pidgin:pidgin:2.7.10:****:*:*:
cpe:2.3:a:pidgin:pidgin:2.7.11:****:*:*:
cpe:2.3:a:pidgin:pidgin:2.7.2:****:*:*:
cpe:2.3:a:pidgin:pidgin:2.7.3:****:*:*:
cpe:2.3:a:pidgin:pidgin:2.7.4:****:*:*:
cpe:2.3:a:pidgin:pidgin:2.7.5:****:*:*:
cpe:2.3:a:pidgin:pidgin:2.7.6:****:*:*:
cpe:2.3:a:pidgin:pidgin:2.7.7:****:*:*:
cpe:2.3:a:pidgin:pidgin:2.7.8:****:*:*:
cpe:2.3:a:pidgin:pidgin:2.7.9:****:*:*:
cpe:2.3:a:pidgin:pidgin:2.8.0:****:*:*:
cpe:2.3:a:pidgin:pidgin:2.9.0:****:*:*:
cpe:2.3:a:pidgin:pidgin:****:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

© CVE.report 2023 |

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