

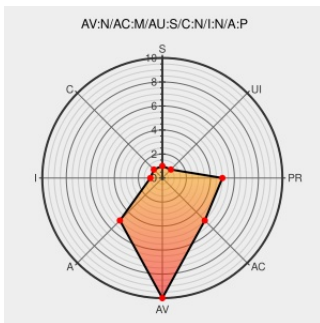


CVE-2012-2214

Published on: 07/03/2012 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:25 PM UTC

CVE-2012-2214

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

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

proxy.c in libpurple in Pidgin before 2.10.4 does not properly handle canceled SOCKS5 connection attempts, which allows user-assisted remote authenticated users to cause a denial of service (application crash) via a sequence of XMPP file-transfer requests.

CVE-2012-2214 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **3.5 - LOW**

Access
Vector

NETWORK

Access
Complexity

MEDIUM

Authentication

SINGLE

Confidentiality
Impact

NONE

Integrity
Impact

NONE

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

mandriva.com

www.mandriva.com
[text/html](#)

[MANDRIVA MDVSA-2012:082](#)

Repository / Oval Repository

oval.cisecurity.org
[text/html](#)

[OVAL oval:org.mitre.oval:def:17886](#)

pidgin/main: changeset 5f9d676cefdb

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

[CONFIRM hg.pidgin.im/pidgin/main/rev/5f9d676cefdb](#)

Pidgin Security Advisories

[Patch](#)
[Vendor Advisory](#)
web.archive.org
[text/html](#)
[Inactive Link](#) [Not Archived](#)

[CONFIRM pidgin.im/news/security/?id=62](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that

By selecting these links, you may be leaving CVEreport's website. We have provided these links to external resources 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	2.2.0	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	2.2.0	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	2.4.0	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:2.2.0:*****:
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:*****:

```

vpe.2.0.a.plugin.plugin.2.0.0. . . . .

```

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:2.2.0:*:*:*:*:*:*:
```

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→](#)