



CVE-2014-0020

Published on: 02/06/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:56 PM UTC

CVE-2014-0020

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

The IRC protocol plugin in libpurple in Pidgin before 2.10.8 does not validate argument counts, which allows remote IRC servers to cause a denial of service (application crash) via a crafted message.

CVE-2014-0020 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

**Access
Vector**

**Access
Complexity**

Authentication

NETWORK

LOW

NONE

**Confidentiality
Impact**

**Integrity
Impact**

**Availability
Impact**

NONE

NONE

PARTIAL

CVE References

Description

Tags

Link

pidgin/main: changeset 9f132a6855cd

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

[CONFIRM](#)
[hg.pidgin.im/pidgin/main/rev/9f132a6855cd](#)

openSUSE-SU-2014:0326-1: moderate: update for pidgin

[lists.opensuse.org](#)
[text/html](#)

[SUSE openSUSE-SU-2014:0326](#)

pidgin/main: changeset 5845d9fa7084

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

[CONFIRM](#)
[hg.pidgin.im/pidgin/main/rev/5845d9fa7084](#)

pidgin/main: changeset 4d9be297d399

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

[CONFIRM](#)
[hg.pidgin.im/pidgin/main/rev/4d9be297d399](#)

Debian -- Security Information -- DSA-2859-1 pidgin

[www.debian.org](#)
[Deprecated Link](#)
[text/html](#)

[DEBIAN DSA-2859](#)

pidgin/main: changeset 6b0e0566af20

[hg.pidgin.im](#)

[CONFIRM](#)

	text/xml	hg.pidgin.im/pidgin/main/rev/6b0e0566af20
Pidgin Security Advisories	Vendor Advisory web.archive.org text/html Inactive Link Not Archived	 CONFIRM pidgin.im/news/security/?id=85
pidgin/main: changeset 7d0fb0c6d8d4	hg.pidgin.im text/xml	 CONFIRM hg.pidgin.im/pidgin/main/rev/7d0fb0c6d8d4
openSUSE-SU-2014:0239-1: moderate: update for pidgin, pidgin-branding-op	lists.opensuse.org text/html	 SUSE openSUSE-SU-2014:0239
USN-2100-1: Pidgin vulnerabilities Ubuntu	www.ubuntu.com text/html	 UBUNTU USN-2100-1
pidgin/main: changeset a167504359e5	hg.pidgin.im text/xml	 CONFIRM hg.pidgin.im/pidgin/main/rev/a167504359e5
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2014:0139

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	2.10.4	All	All	All
Application	Pidgin	Pidgin	2.10.5	All	All	All
Application	Pidgin	Pidgin	2.10.6	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	2.6.3	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	2.10.4	All	All	All
Application	Pidgin	Pidgin	2.10.5	All	All	All
Application	Pidgin	Pidgin	2.10.6	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	2.6.3	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:2.10.4:*****:*						
cpe:2.3:a:pidgin:pidgin:2.10.5:*****:*						
cpe:2.3:a:pidgin:pidgin:2.10.6:*****:*						
cpe:2.3:a:pidgin:pidgin:2.2.0:*****:*						
cpe:2.3:a:pidgin:pidgin:2.2.1:*****:*						

[illegible]

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:2.10.4:*:*:*:*:*:*:
```

cpe:2.3:a:pidgin:pidgin:2.10.5:*:*:*:*:*:*:

cpe:2.3:a:pidgin:pidgin:2.10.6:*:*:*:*:*:*:

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:2.6.3:*:*:*:*:*:*:

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](#)