



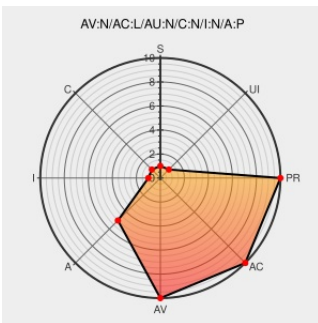
Last Modified on: 03/23/2021 11:25:22 PM UTC

CVE-2009-4881

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF 

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

Integer overflow in the `__vstrfmon_l` function in `stdlib/strfmon_l.c` in the `strfmon` implementation in the GNU C Library (aka `glibc` or `libc6`) before 2.10.1 allows context-dependent attackers to cause a denial of service (application crash) via a crafted format string, as demonstrated by the `%99999999999999999999n` string, a related issue to `CVE-2008-1391`.

CVE-2009-4881 has been assigned by  cve@mitre.org 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
Gentoo Linux Documentation -- GNU C library: Multiple vulnerabilities	security.gentoo.org text/html	 GENTOO GLSA-201011-01
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	 XF gnuclibrary-vstrfmonl-overflow(59241)
Debian -- Security Information -- DSA-2058-1 glibc, eglibc	www.debian.org Deprecated Link text/html	 DEBIAN DSA-2058
Support / Security / Advisories / / MDVSA-2010:111 Mandriva	www.mandriva.com text/html	 MANDRIVA MDVSA-2010:111
10600 – (CVE-2008-1391) stdio/strfmon.c multiple vulnerabilities (CVE-2008-1391)	sources.redhat.com text/html	 CONFIRM sources.redhat.com/bugzilla/show_bug.cgi?id=10600

sourceware.org Git -
glibc.git/commit

Patch
sourceware.org
text/xml

 CONFIRM sourceware.org/git/?p=glibc.git;a=commit;h=153aa31b93be22e01b236375fb02a9fb9a0195f

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	Gnu	Glibc	1.00	All	All	All
Application	Gnu	Glibc	1.01	All	All	All
Application	Gnu	Glibc	1.02	All	All	All
Application	Gnu	Glibc	1.03	All	All	All
Application	Gnu	Glibc	1.04	All	All	All
Application	Gnu	Glibc	1.05	All	All	All
Application	Gnu	Glibc	1.06	All	All	All
Application	Gnu	Glibc	1.07	All	All	All
Application	Gnu	Glibc	1.08	All	All	All
Application	Gnu	Glibc	1.09	All	All	All
Application	Gnu	Glibc	2.0	All	All	All
Application	Gnu	Glibc	2.0.1	All	All	All
Application	Gnu	Glibc	2.0.2	All	All	All
Application	Gnu	Glibc	2.0.3	All	All	All
Application	Gnu	Glibc	2.0.4	All	All	All
Application	Gnu	Glibc	2.0.5	All	All	All
Application	Gnu	Glibc	2.0.6	All	All	All
Application	Gnu	Glibc	2.1	All	All	All
Application	Gnu	Glibc	2.1.1	All	All	All
Application	Gnu	Glibc	2.1.1.6	All	All	All
Application	Gnu	Glibc	2.1.2	All	All	All
Application	Gnu	Glibc	2.1.3	All	All	All
Application	Gnu	Glibc	2.1.3.10	All	All	All
Application	Gnu	Glibc	2.1.9	All	All	All
Application	Gnu	Glibc	2.2	All	All	All

Application	Gnu	Glibc	2.2.1	All	All	All
Application	Gnu	Glibc	2.2.2	All	All	All
Application	Gnu	Glibc	2.2.3	All	All	All
Application	Gnu	Glibc	2.2.4	All	All	All
Application	Gnu	Glibc	2.2.5	All	All	All
Application	Gnu	Glibc	2.3	All	All	All
Application	Gnu	Glibc	2.3.1	All	All	All
Application	Gnu	Glibc	2.3.10	All	All	All
Application	Gnu	Glibc	2.3.2	All	All	All
Application	Gnu	Glibc	2.3.3	All	All	All
Application	Gnu	Glibc	2.3.4	All	All	All
Application	Gnu	Glibc	2.3.5	All	All	All
Application	Gnu	Glibc	2.3.6	All	All	All
Application	Gnu	Glibc	2.4	All	All	All
Application	Gnu	Glibc	2.5	All	All	All
Application	Gnu	Glibc	2.5.1	All	All	All
Application	Gnu	Glibc	2.6	All	All	All
Application	Gnu	Glibc	2.6.1	All	All	All
Application	Gnu	Glibc	2.7	All	All	All
Application	Gnu	Glibc	2.8	All	All	All
Application	Gnu	Glibc	1.00	All	All	All
Application	Gnu	Glibc	1.01	All	All	All
Application	Gnu	Glibc	1.02	All	All	All
Application	Gnu	Glibc	1.03	All	All	All
Application	Gnu	Glibc	1.04	All	All	All
Application	Gnu	Glibc	1.05	All	All	All
Application	Gnu	Glibc	1.06	All	All	All
Application	Gnu	Glibc	1.07	All	All	All
Application	Gnu	Glibc	1.08	All	All	All
Application	Gnu	Glibc	1.09	All	All	All
Application	Gnu	Glibc	2.0	All	All	All
Application	Gnu	Glibc	2.0.1	All	All	All
Application	Gnu	Glibc	2.0.2	All	All	All
Application	Gnu	Glibc	2.0.3	All	All	All
Application	Gnu	Glibc	2.0.4	All	All	All
Application	Gnu	Glibc	2.0.5	All	All	All

Application	Gnu	Glibc	2.0.5	All	All	All
Application	Gnu	Glibc	2.0.6	All	All	All
Application	Gnu	Glibc	2.1	All	All	All
Application	Gnu	Glibc	2.1.1	All	All	All
Application	Gnu	Glibc	2.1.1.6	All	All	All
Application	Gnu	Glibc	2.1.2	All	All	All
Application	Gnu	Glibc	2.1.3	All	All	All
Application	Gnu	Glibc	2.1.3.10	All	All	All
Application	Gnu	Glibc	2.1.9	All	All	All
Application	Gnu	Glibc	2.2	All	All	All
Application	Gnu	Glibc	2.2.1	All	All	All
Application	Gnu	Glibc	2.2.2	All	All	All
Application	Gnu	Glibc	2.2.3	All	All	All
Application	Gnu	Glibc	2.2.4	All	All	All
Application	Gnu	Glibc	2.2.5	All	All	All
Application	Gnu	Glibc	2.3	All	All	All
Application	Gnu	Glibc	2.3.1	All	All	All
Application	Gnu	Glibc	2.3.10	All	All	All
Application	Gnu	Glibc	2.3.2	All	All	All
Application	Gnu	Glibc	2.3.3	All	All	All
Application	Gnu	Glibc	2.3.4	All	All	All
Application	Gnu	Glibc	2.3.5	All	All	All
Application	Gnu	Glibc	2.3.6	All	All	All
Application	Gnu	Glibc	2.4	All	All	All
Application	Gnu	Glibc	2.5	All	All	All
Application	Gnu	Glibc	2.5.1	All	All	All
Application	Gnu	Glibc	2.6	All	All	All
Application	Gnu	Glibc	2.6.1	All	All	All
Application	Gnu	Glibc	2.7	All	All	All
Application	Gnu	Glibc	2.8	All	All	All
Application	Gnu	Glibc	All	All	All	All
cpe:2.3:a:gnu:glibc:1.00:*****:						
cpe:2.3:a:gnu:glibc:1.01:*****:						
cpe:2.3:a:gnu:glibc:1.02:*****:						
cpe:2.3:a:gnu:glibc:1.03:*****:						

cpe:2.3:a:gnu:glibc:1.04:*****:
cpe:2.3:a:gnu:glibc:1.05:*****:
cpe:2.3:a:gnu:glibc:1.06:*****:
cpe:2.3:a:gnu:glibc:1.07:*****:
cpe:2.3:a:gnu:glibc:1.08:*****:
cpe:2.3:a:gnu:glibc:1.09:*****:
cpe:2.3:a:gnu:glibc:2.0:*****:
cpe:2.3:a:gnu:glibc:2.0.1:*****:
cpe:2.3:a:gnu:glibc:2.0.2:*****:
cpe:2.3:a:gnu:glibc:2.0.3:*****:
cpe:2.3:a:gnu:glibc:2.0.4:*****:
cpe:2.3:a:gnu:glibc:2.0.5:*****:
cpe:2.3:a:gnu:glibc:2.0.6:*****:
cpe:2.3:a:gnu:glibc:2.1:*****:
cpe:2.3:a:gnu:glibc:2.1.1:*****:
cpe:2.3:a:gnu:glibc:2.1.1.6:*****:
cpe:2.3:a:gnu:glibc:2.1.2:*****:
cpe:2.3:a:gnu:glibc:2.1.3:*****:
cpe:2.3:a:gnu:glibc:2.1.3.10:*****:
cpe:2.3:a:gnu:glibc:2.1.9:*****:
cpe:2.3:a:gnu:glibc:2.2:*****:
cpe:2.3:a:gnu:glibc:2.2.1:*****:
cpe:2.3:a:gnu:glibc:2.2.2:*****:
cpe:2.3:a:gnu:glibc:2.2.3:*****:
cpe:2.3:a:gnu:glibc:2.2.4:*****:
cpe:2.3:a:gnu:glibc:2.2.5:*****:
cpe:2.3:a:gnu:glibc:2.3:*****:
cpe:2.3:a:gnu:glibc:2.3.1:*****:

cpe:2.3:a:gnu:glibc:2.3.10:*****:
cpe:2.3:a:gnu:glibc:2.3.2:*****:
cpe:2.3:a:gnu:glibc:2.3.3:*****:
cpe:2.3:a:gnu:glibc:2.3.4:*****:
cpe:2.3:a:gnu:glibc:2.3.5:*****:
cpe:2.3:a:gnu:glibc:2.3.6:*****:
cpe:2.3:a:gnu:glibc:2.4:*****:
cpe:2.3:a:gnu:glibc:2.5:*****:
cpe:2.3:a:gnu:glibc:2.5.1:*****:
cpe:2.3:a:gnu:glibc:2.6:*****:
cpe:2.3:a:gnu:glibc:2.6.1:*****:
cpe:2.3:a:gnu:glibc:2.7:*****:
cpe:2.3:a:gnu:glibc:2.8:*****:
cpe:2.3:a:gnu:glibc:1.00:*****:
cpe:2.3:a:gnu:glibc:1.01:*****:
cpe:2.3:a:gnu:glibc:1.02:*****:
cpe:2.3:a:gnu:glibc:1.03:*****:
cpe:2.3:a:gnu:glibc:1.04:*****:
cpe:2.3:a:gnu:glibc:1.05:*****:
cpe:2.3:a:gnu:glibc:1.06:*****:
cpe:2.3:a:gnu:glibc:1.07:*****:
cpe:2.3:a:gnu:glibc:1.08:*****:
cpe:2.3:a:gnu:glibc:1.09:*****:
cpe:2.3:a:gnu:glibc:2.0:*****:
cpe:2.3:a:gnu:glibc:2.0.1:*****:
cpe:2.3:a:gnu:glibc:2.0.2:*****:
cpe:2.3:a:gnu:glibc:2.0.3:*****:
cpe:2.3:a:gnu:glibc:2.0.4:*****:
cpe:2.3:a:gnu:glibc:2.0.5:*****:

```
cpe:2.3:a:gnu:glibc:2.0.6:*:*:*:*:*:*:
```

```
cpe:2.3:a:gnu:glibc:2.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:gnu:glibc:2.1.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:gnu:glibc:2.1.1.6:*:*:*:*:*:*:
```

```
cpe:2.3:a:gnu:glibc:2.1.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:gnu:glibc:2.1.3:*:*:*:*:*:*:
```

```
cpe:2.3:a:gnu:glibc:2.1.3.10:*:*:*:*:*:*:
```

cpe:2.3:a:gnu:glibc:2.1.9:*:*:*:*:*:*:*

```
cpe:2.3:a:gnu:glibc:2.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:gnu:glibc:2.2.1:*:*:*:*:*:*:*:
```

```
cpe:2.3:a:gnu:glibc:2.2.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:gnu:glibc:2.2.3:*:*:*:*:*:*:*:
```

```
cpe:2.3:a:gnu:glibc:2.2.4:*:*:*:*:*:*:
```

```
cpe:2.3:a:gnu:glibc:2.2.5:*:*:*:*:*:*:
```

```
cpe:2.3:a:gnu:glibc:2.3:*:*:*:*:*:*:*:
```

```
cpe:2.3:a:gnu:glibc:2.3.1:*:*:*:*:*:*:*:
```

```
cpe:2.3:a:gnu:glibc:2.3.10:*:*:*:*:*:*:
```

```
cpe:2.3:a:gnu:glibc:2.3.2:*:*:*:*:*:
```

```
cpe:2.3:a:gnu:glibc:2.3.3:*:*:*:*:*:*:
```

```
cpe:2.3:a:gnu:glibc:2.3.4:*:*:*:*:*:*:
```

```
cpe:2.3:a:gnu:glibc:2.3.5:*:*:*:*:*:*:
```

cpe:2.3:a:gnu:glibc:2.3.6:*:*:*:*:*:*:*

```
cpe:2.3:a:gnu:glibc:2.4:*:*:*:*:*:
```

```
cpe:2.3:a:gnu:glibc:2.5:*:*:*:*:*:
```

```
cpe:2.3:a:gnu:glibc:2.5.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:gnu:glibc:2.6:*:*:*:*:*:*:
```

```
cpe:2.3:a:gnu:glibc:2.6.1:*.:*:*:*:*:
```

```
cpe:2.3:a:gnu:glibc:2.7:*:*:*:*:*:
```

cpe:2.3:a:gnu:glibc:2.8:*:*:*:*:*:

cpe:2.3:a:gnu:glibc:*:*:*:*:*:

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](#)