

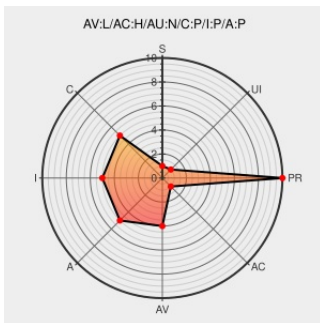


CVE-2011-1658

Published on: 04/08/2011 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:15 PM UTC

CVE-2011-1658

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

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

ld.so in the GNU C Library (aka glibc or libc6) 2.13 and earlier expands the \$ORIGIN dynamic string token when RPATH is composed entirely of this token, which might allow local users to gain privileges by creating a hard link in an arbitrary directory to a (1) setuid or (2) setgid program with this RPATH value, and then executing the program with a crafted value for the LD_PRELOAD environment variable, a different

vulnerability than CVE-2010-3847 and CVE-2011-0536. NOTE: it is not expected that any standard operating-system distribution would ship an applicable setuid or setgid program.

CVE-2011-1658 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **3.7 - LOW**

**Access
Vector**

LOCAL

**Access
Complexity**

HIGH

Authentication

NONE

**Confidentiality
Impact**

PARTIAL

**Integrity
Impact**

PARTIAL

**Availability
Impact**

PARTIAL

CVE References

Description

Tags

Link

Bug 12393 – ld.so: insecure handling of privileged programs' RPATHs with \$ORIGIN

[Patch](#)
[sourceware.org](#)
[text/html](#)

[MISC](#)
[sourceware.org/bugzilla/show_bug.cgi?id=12393](#)

SecurityFocus

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

[BUGTRAQ](#) 20111013 VMSA-2011-0012
VMware ESXi and ESX updates to third party libraries and ESX Service Console

667974 – (CVE-2011-0536) CVE-2011-0536 glibc: CVE-2010-3847 fix causes linker to search CWD when running privileged program with \$ORIGIN in R*PATH

[Patch](#)
[bugzilla.redhat.com](#)
[text/html](#)

[MISC](#) [bugzilla.redhat.com/show_bug.cgi?id=667974](#)

About Secunia Research | Flexera

secunia.com

Deprecated Link

text/plain



SECUNIA 46397

IBM X-Force Exchange

exchange.xforce.ibmcloud.com

text/html



XF gnuclibrary-ldso-priv-esc(66820)

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	1.09.1	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	2.10	All	All	All
Application	Gnu	Glibc	2.10.1	All	All	All
Application	Gnu	Glibc	2.10.2	All	All	All
Application	Gnu	Glibc	2.11	All	All	All
Application	Gnu	Glibc	2.11.1	All	All	All
Application	Gnu	Glibc	2.11.2	All	All	All
Application	Gnu	Glibc	2.11.3	All	All	All
Application	Gnu	Glibc	2.12.0	All	All	All
Application	Gnu	Glibc	2.12.1	All	All	All
Application	Gnu	Glibc	2.12.2	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	2.9	All	All	All
Application	Gnu	Glibc	1.00	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	1.09.1	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	2.10	All	All	All
Application	Gnu	Glibc	2.10.1	All	All	All
Application	Gnu	Glibc	2.10.2	All	All	All
Application	Gnu	Glibc	2.11	All	All	All
Application	Gnu	Glibc	2.11.1	All	All	All
Application	Gnu	Glibc	2.11.2	All	All	All
Application	Gnu	Glibc	2.11.3	All	All	All
Application	Gnu	Glibc	2.12.0	All	All	All
Application	Gnu	Glibc	2.12.1	All	All	All
Application	Gnu	Glibc	2.12.2	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	2.9	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:1.09.1:*****:						

cpe:2.3:a:gnu:glibc:2.0:*:*:*:*:*:
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:2.10:*:*:*:*:*:
cpe:2.3:a:gnu:glibc:2.10.1:*:*:*:*:*:
cpe:2.3:a:gnu:glibc:2.10.2:*:*:*:*:*:
cpe:2.3:a:gnu:glibc:2.11:*:*:*:*:*:
cpe:2.3:a:gnu:glibc:2.11.1:*:*:*:*:*:
cpe:2.3:a:gnu:glibc:2.11.2:*:*:*:*:*:
cpe:2.3:a:gnu:glibc:2.11.3:*:*:*:*:*:
cpe:2.3:a:gnu:glibc:2.12.0:*:*:*:*:*:
cpe:2.3:a:gnu:glibc:2.12.1:*:*:*:*:*:
cpe:2.3:a:gnu:glibc:2.12.2:*:*:*:*:*:
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:2.9:*****:
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:1.00.1:*****:

```
cpe:2.3:a:gnu:glibc:1.09.1:::~::~:
```

```
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:2.10:*:*:*:*:*:*:
```

cpe:2.3:a:gnu:glibc:2.10.1:*:*:*:*:*:*:*

```
cpe:2.3:a:gnu:glibc:2.10.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:gnu:glibc:2.11:*:*:*:*:*:*:
```

```
cpe:2.3:a:gnu:glibc:2.11.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:gnu:glibc:2.11.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:gnu:glibc:2.11.3:*:*:*:*:*:*:
```

```
cpe:2.3:a:gnu:glibc:2.12.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:gnu:glibc:2.12.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:gnu:glibc:2.12.2:*:*:*:*:*:*:
```

```
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:2.9:*****:
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