Critical: glibc security and bug fix update - CVE-2015-7547

Sanjay Naikwadi - 2016-02-23 - 0 Comments - in Security Advisory & Bulletins

Critical: glibc security and bug fix update - CVE-2015-7547

Release	Classification	Level	DB Platform	Categories
All	Solution		ALL	Security

SYMPTOM

GNU glibc contains a buffer overflow vulnerability in the DNS resolver, which may allow a

remote attacker to execute arbitrary code.

More details and analysis are available in the patch announcement from `glibc` developers.

The getaddrinfo() function allows a buffer overflow condition in which arbitrary code may be

executed. The impact may vary depending on if the use case is local or remote.

CWE-121: Stack-based Buffer Overflow - CVE-2015-7547 According to glibc developers, the vulnerable code was initially added in May 2008 as part of the development forglibc 2.9. All versions from 2.9 (originally released November 2008) to 2.22 appear to be affected.

FIX/WORKAROUND

DO NOT perform an update of the entire system.

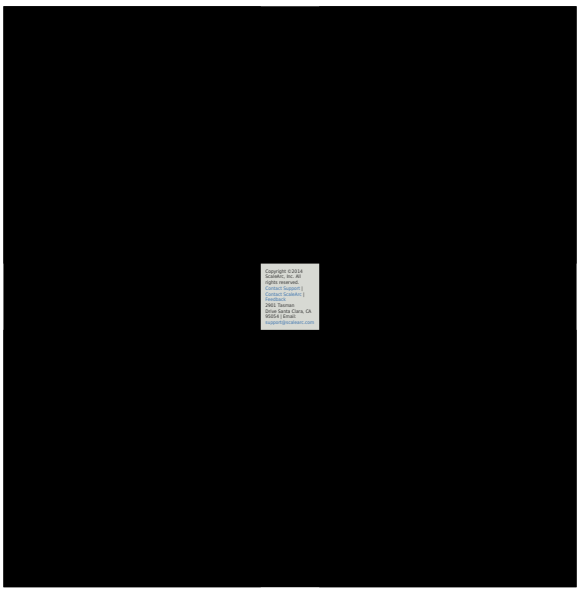
Login to ScaleArc box with idb user and download the following rpms in /tmp directory and

Verify your exisiting version of glibc

```
[idb@scalearc-1 tmp]$ rpm -qa |grep glibc
glibc-common-2.12-1.149.el6_6.5.x86_64
glibc-2.12-1.149.el6_6.5.x86_64

cd /tmp

curl -O
"https://idblb-iso.s3.amazonaws.com/Patch_Upgrades/Glibc/glibc-2.12-1.166.el6_7.7.x86_64.rpm"
curl -O
"https://idblb-iso.s3.amazonaws.com/Patch_Upgrades/Glibc/glibc-common-2.12-1.166.el6_7.7.x86_64.rpm"

Verify the md5sum :
4b5abcc64f1577bcc891726d47ae0d7c  glibc-2.12-1.166.el6_7.7.x86_64.rpm
a5d2e83706d8bc1be1e2f09f320bd9c6  glibc-common-2.12-1.166.el6_7.7.x86_64.rpm

Install the rpms :
sudo rpm -Uvh glibc*

Verify the glibc version

[idb@scalearc-1 tmp]$ rpm -qa |grep glibc
glibc-common-2.12-1.166.el6_7.7.x86_64
glibc-2.12-1.166.el6_7.7.x86_64
```

If you are experiencing issues with ScaleArc or with any of it's features, please contact ScaleArc Support. We are available 24x7 by phone at 855 800 7225 or +1 408 412 7315.

For general support inquiries, you can also e-mail us at support@scalearc.com.



Permalink:
https://support.scalearc.com/kb/articles/3084