DDN STORAGE

TECHNICAL SUPPORT BULLETIN

DDN TECHNICAL SUPPORT | SPT-TSB-0051 (A4) | 11 APRIL 2016

CVE-2015-7547 Security Vulnerability in DNS Resolver of GNU C Library

Issue Summary

The GNU C Library (glibc) is a portable, internationalized, standards-compliant, high-performance C library used in most Linux distributions. Many DDN products include a Linux kernel that uses glibc.

DDN has learned that in several versions of glibc, the client-side DNS resolver is susceptible to remote attack. When the `getaddrinfo()`function in the resolver library is used, a remote attacker can send a crafted DNS response to the resolver and cause it to crash or to execute code with the permissions of the user running the library.

Versions 2.9 through 2.22 of glibc are affected by this vulnerability. Version 2.23 resolves this issue.

Technical Background

In affected versions of glibc, the client-side DNS resolver, `libresolv`, is vulnerable to a buffer overflow exploit due to the way it performs parallel DNS queries for A and AAAA. This issue is exposed only when `libresolv` is called from the Name Service Switch (NSS) service module, `nss_dns`, which uses the resolver to perform DNS lookups using the `getaddrinfo()` library function. (These lookups provide translation between host names and IP addresses.)

Software using this function may be exploited with attacker-controlled domain names, attacker-controlled DNS servers, or through a man-in-the-middle attack. Note that the Name Service Cache Daemon, `ncsd`, is one such affected software module.

Buffer management was simplified in glibc version 2.23 to remove the overflow. The `nscd` daemon was updated for compatibility with the new version of glibc.

Determining Vulnerability

A system is exposed to the DNS resolver buffer overflow exploit in affected versions of glibc if the `dns` service modules are listed in `/etc/nsswitch.conf`.

Removing these modules will mitigate the exploit. However, it will then become impossible to perform DNS lookups using the standard glibc name resolution functions. Consequently, such a mitigation is rarely useful.

Affected DDN Products

DDN has evaluated all currently supported products for vulnerability to this glibc exploit. The results of that evaluation are detailed below.

Not Affected by Glibc Vulnerability

The following DDN products are ***NOT*** affected by the glibc DNS resolver vulnerability:

- SFA OS, SFA14K, SFA12K, SFA10K, SFA7700, S2A6620
- S2A DirectOS, S2A9900
- IME, IME14K
- EXAScaler Bridge, GRIDScaler Bridge (formerly WOS Bridge)

Affected by Glibc Vulnerability

DDN products affected by the glibc DNS resolver vulnerability, as well as product upgrades that remove this vulnerability, are listed in the table below. Recommendations for addressing the vulnerability are provided for each affected product version.

PRODUCT	VERSION	RESOLUTION
DirectMon	2.4	Contact DDN Support to obtain a patch.
EXAScaler	2.3.1	Includes updated glibc. GA expected April 2016.
EXAScaler	2.2.0	Upgrade to 2.3.1. Do not update glibc or nscd directly.
EXAScaler	2.1.2	Upgrade to 2.3.1. Do not update glibc or nscd directly.
EXAScaler	2.0.3	Upgrade to 2.3.1. Do not update glibc or nscd directly.
GRIDScaler	3.2.1	Includes updated glibc. No further action required.
GRIDScaler - RHEL	3.2.0	• *Option 1* – Upgrade to 3.2.1. • *Option 2* - Contact DDN Support for rpm package with updated glibc.
GRIDScaler - CentOS	3.2.0	• *Option 1* – Upgrade to 3.2.1. • *Option 2* - Contact DDN Support for rpm package with updated glibc.
GRIDScaler - OEL	3.2.0	• *Option 1* – Upgrade to 3.2.1. • *Option 2* - Contact DDN Support for rpm package with updated glibc.
GRIDScaler - RHEL	3.1.0	Upgrade to 3.2.1. Do not update glibc or nscd directly.
GRIDScaler - RHEL	3.0.0	Upgrade to 3.2.1. Do not update glibc or nscd directly.
GRIDScaler - CentOS	2.1.2	Upgrade to 3.2.1. Do not update glibc or nscd directly.
MEDIAScaler	All	Update GRIDScaler as above.
WOS Access CIFS NFS	1.6.0	Includes updated glibc & nscd. GA expected June 2016.
WOS Access CIFS NFS	1.5.x	Upgrade to 1.6.0. Do not update glibc or nscd directly.

PRODUCT	VERSION	RESOLUTION
WOS Access CIFS NFS	1.4.x	Upgrade to 1.6.0. Do not update glibc or nscd directly.
WOS Access S3 Swift	2.2.0	Includes updated glibc & nscd. GA expected May 2016.
WOS Access S3 Swift	2.1.x	Upgrade to 2.2.0. Do not update glibc or nscd directly.
WOS Access S3 Swift	2.0.x	• *Option 1* – Upgrade to 2.2.0. • *Option 2* – Install updated glibc & nscd packages.
WOS Core	2.6.0	Includes updated glibc & nscd. GA expected June 2016.
WOS Core	2.5.4	• *Option 1* – Upgrade to 2.6.0. • *Option 2* – Contact DDN Support for glibc and ncsd patch instructions. **ALERT! Do *NOT* attempt patch without DDN assistance!** • *Option 3* – Turn off setting that configures cluster DNS servers to enable hostnames in addition to IP addresses.
WOS Core	2.5.3	• *Option 1* – Upgrade to 2.6.0. Do not update glibc or nscd directly. • *Option 2* – Turn off setting that configures cluster DNS servers to enable hostnames in addition to IP addresses.

Updating the Linux Kernel

With some versions of some DDN products, you can eliminate the possibility of a glibc DNS resolver exploit by updating glibc and the Name Server Cache Demon (nscd) directly in the Linux kernel. Instructions for Red Hat and CentOS kernel updates are provided below.

ALERT! Do ***NOT*** use this procedure this unless recommended in the table above or instructed to do so by a DDN Support engineer. Directly updating modules in the Linux kernel may create incompatibilities with your DDN software.

ALERT! Do ***NOT*** use this procedure with WOS Core. ***Contact DDN Support for assistance*** if you wish to patch glibc and nscd in WOS Core 2.5.4.

Step 1. Update the glibc and ncsd packages on your system using the packages released with the following errata:

Red Hat Enterprise Linux

RHEL Desktop	v 6	https://rhn.redhat.com/errata/RHSA-2016-0175.html
RHEL Desktop	v 7	https://rhn.redhat.com/errata/RHSA-2016-0176.html
RHEL HPC Node	v 6	https://rhn.redhat.com/errata/RHSA-2016-0175.html
RHEL HPC Node	v 7	https://rhn.redhat.com/errata/RHSA-2016-0176.html
RHEL Server	v 6	https://rhn.redhat.com/errata/RHSA-2016-0175.html
RHEL Server	v 7	https://rhn.redhat.com/errata/RHSA-2016-0176.html
RHEL Server AUS	v 6.2	https://rhn.redhat.com/errata/RHSA-2016-0225.html
RHEL Server AUS	v 6.4	https://rhn.redhat.com/errata/RHSA-2016-0225.html
RHEL Server AUS	v 6.5	https://rhn.redhat.com/errata/RHSA-2016-0225.html
RHEL Server EUS	v 6.4.z	https://rhn.redhat.com/errata/RHSA-2016-0225.html
RHEL Server EUS	v 6.5.z	https://rhn.redhat.com/errata/RHSA-2016-0225.html
RHEL Server EUS	v 6.6.z	https://rhn.redhat.com/errata/RHSA-2016-0225.html
RHEL Workstation	v 6	https://rhn.redhat.com/errata/RHSA-2016-0175.html

RHEL Workstation	v 7	https://rhn.redhat.com/errata/RHSA-2016-0176.html
RHEL	v 5	Not affected. No action required.

CentOS Linux v 6 for x86_64 (64 bit)

Errata	https://lists.centos.org/pipermail/centos-announce/2016-February/021668.html
Mirror	http://mirror.centos.org/centos/6/updates/x86_64/Packages/
RPM Packages	glibc-2.12-1.166.el6_7.7.i686.rpm glibc-2.12-1.166.el6_7.7.x86_64.rpm glibc-common-2.12-1.166.el6_7.7.x86_64.rpm glibc-devel-2.12-1.166.el6_7.7.i686.rpm glibc-devel-2.12-1.166.el6_7.7.x86_64.rpm glibc-headers-2.12-1.166.el6_7.7.x86_64.rpm glibc-static-2.12-1.166.el6_7.7.i686.rpm glibc-static-2.12-1.166.el6_7.7.x86_64.rpm glibc-utils-2.12-1.166.el6_7.7.x86_64.rpm nscd-2.12-1.166.el6_7.7.x86_64.rpm

Step 2. Reboot the system.

NOTE Because this vulnerability affects so many applications on the system, the safest and recommended way to assure that every application uses the updated glibc packages is to restart the system.

Contacting DDN Technical Support

Please contact DDN Technical Support at any time if you have questions or require assistance. Support can be reached by phone, by email, or on the web as listed below.

Web

DDN Community Support Portal	https://community.ddn.com/login
Portal Assistance	webportal.support@ddn.com

Telephone

DDN Support Worldwide Directory	http://www.ddn.com/support/contact-support

Email

Support Email	support@ddn.com

Bulletins

Support Bulletins	http://www.ddn.com/support/technical-support-bulletins
End-of-Life Notices	http://www.ddn.com/support/end-of-life-notices
Bulletin Subscription Requests	support-tsb@ddn.com