



**State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory**

February 18, 2016

The following cyber advisory was issued by the State of Alaska and was intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

ADVISORY NUMBER:

SA2016-033

DATE(S) ISSUED:

02/18/2016

SUBJECT:

Multiple Vulnerabilities in GNU C Library Could Allow for Arbitrary Code Execution

OVERVIEW:

Multiple vulnerabilities has been discovered in the GNU C Library (glibc), which could allow for arbitrary code execution. This library is required in all modern distributions of Linux as it defines the system calls and other basic facilities used in the Linux kernel. Successful exploitation of this vulnerability could result in an attacker gaining the same privileges as the exploited application. Depending on the privileges associated with the application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts could lead to a denial of service condition for the affected application.

THREAT INTELLIGENCE:

A proof of concept has been publicly released. There are currently no reports of this vulnerability being exploited in the wild.

SYSTEMS AFFECTED:

GNU C Library (glibc) versions 2.9 through 2.22 which may affect most Linux-based systems and applications compiled with glibc.

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

TECHNICAL SUMMARY:

Multiple vulnerabilities in GNU C Library (glibc) could allow for arbitrary code execution

- An arbitrary code execution vulnerability exists in the host name resolver 'getaddrinfo' function due to a stack-based buffer overflow (CVE-2015-7547).
- A denial of service vulnerability exists in the 'nss_files database' (CVE-2014-8121).
- A buffer overflow vulnerability exists in the '_r variants' host name resolution functions which may result in arbitrary code execution (CVE-2015-1781).
- An information leak vulnerability exists in 'strftime' (CVE-2015-8776).
- A security bypass vulnerability exists in LD_POINTER_GUARD (CVE-2015-8777).
- A denial of service vulnerability exists in the 'hcreate' and 'hcreate_r functions' due to a failed bounds check (CVE-2015-8778).
- A denial of service vulnerability exists in 'catopen' due to several unbound stack allocations (CVE-2015-8779).
- An arbitrary code execution vulnerability exists in 'strxfrm' due to an integer overflow.

- A denial of service vulnerability exists in the 'nmatch' function when processing NUL character of a malformed pattern.
- A heap-based buffer overflow exists in the IO_wstr_overflow function.
- A denial of service vulnerability exists in the '_nss_dns_gethostbyname4_r' function' which may result in a memory leak.

An attacker can exploit these vulnerabilities to execute arbitrary code in the context of the affected application. Successful exploitation of these vulnerabilities may result in an attacker gaining the same privileges as the exploited application. Depending on the privileges associated with the application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts could lead to a denial of service condition for the affected application.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply appropriate patches provided by the affected Linux distribution to the vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user to diminish the effects of a successful attack.
- Contact device vendors to determine if equipment on your infrastructure is affected.
- Review internal applications to determine if they were compiled with the vulnerable versions of glibc.
- Temporary mitigation techniques include
 - Dropping all UDP DNS packets greater than 512 bytes at the firewall.
 - A local resolver (that drops non-compliant responses).
 - Avoid dual A and AAAA queries
 - Prohibit use of `options edns0` in /etc/resolv.conf
 - Limit all TCP replies to 1024 bytes.

REFERENCES:

Sourceware:

<https://sourceware.org/ml/libc-alpha/2016-02/msg00416.html>

Google Online Security Blog:

<https://googleonlinesecurity.blogspot.com/2016/02/cve-2015-7547-glibc-getaddrinfo-stack.html>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8121>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1781>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7547>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8776>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8777>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8778>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8779>

SecurityFocus:

<http://www.securityfocus.com/archive/1/537534/30/0/threaded>