

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is 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.

TLP:WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

<http://www.us-cert.gov/tlp/>

DATE(S) ISSUED:

01/28/2015

SUBJECT:

Vulnerability in GNU C Library Could Allow for Remote Code Execution (Ghost Vulnerability)

EXECUTIVE SUMMARY:

A vulnerability has been discovered in the GNU C Library (glibc) which could allow for remote 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:

As of the writing of this advisory, no exploit code is available. This vulnerability is known as the Ghost vulnerability in public sources.

SYSTEM AFFECTED:

- Debian 6.0
- Debian 7.0
- SuSE Linux 7.1.0
- WireX Immunix OS 7+
- Red Hat Enterprise Linux 5
- Red Hat Enterprise Linux 6
- Red Hat Enterprise Linux 7
- Oracle Enterprise Linux 5
- CentOS 6
- CentOS 7
- Ubuntu 10.04
- Ubuntu 12.04

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: Medium

TECHNICAL SUMMARY:

Glibc is prone to a heap-based buffer overflow vulnerability because it fails to properly sanitize user-supplied data before copying it into the buffer. Specifically, this issue exists in the `'__nss_hostname_digits_dots()'` function, which is used by the `'gethostbyname()'` and `'gethostbyname2()'` function calls. As this vulnerability is triggered by the `gethostbyname*()` function calls, this vulnerability has been dubbed GHOST, for GetHOST. The first vulnerable version of glibc is glibc-2.2. This vulnerability was fixed on May 21, 2013 between the releases of glibc-2.17 and glibc-2.18, however because it was not recognized as a security threat, most stable distributions were left exposed.

An attacker can exploit this vulnerability to execute arbitrary code in the context of the affected application. 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.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by the affected Linux distribution to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:

Qualys:

<https://community.qualys.com/blogs/laws-of-vulnerabilities/2015/01/27/the-ghost-vulnerability>
<https://www.qualys.com/research/security-advisories/GHOST-CVE-2015-0235.txt>

Red Hat:

<https://rhn.redhat.com/errata/RHSA-2015-0090.html>

Debian:

<https://security-tracker.debian.org/tracker/CVE-2015-0235>

Ubuntu:

<https://launchpad.net/ubuntu/+source/eglibc>

GNU:

<http://www.gnu.org/software/libc/>

Security Focus:

<http://www.securityfocus.com/bid/72325>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0235>

TLP:WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

<http://www.us-cert.gov/tlp/>