

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.

DATE(S) ISSUED:

04/02/2013

SUBJECT:

Maliciously Crafted Regular Expression Can Cause Memory Exhaustion in named (BIND)

OVERVIEW:

ISC BIND contains a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition.

SYSTEMS AFFECTED:

- BIND 9.7 running on UNIX platforms
- BIND 9.8.0--9.8.5b1 running on UNIX platforms
- BIND 9.9.0-9.9.3b1 running on UNIX platforms

RISK:

Government:

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

Businesses:

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

Home users: **Low**

DESCRIPTION:

A flaw in a library used by BIND 9.7, 9.8, and 9.9, when compiled on Unix and related operating systems, allows an attacker to deliberately cause excessive memory consumption by the named process, potentially resulting in exhaustion of memory resources on the affected server. This condition can crash BIND 9 and will likely severely affect operation of other programs running on the same machine.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches to vulnerable systems immediately after appropriate testing. If testing reveals patching isn't acceptable, consider implementing the workaround described by the ISC or the appropriate UNIX vendor.

References:

ISC:

<https://kb.isc.org/article/AA-00871>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2266>

Cisco:

<http://tools.cisco.com/security/center/viewAlert.x?alertId=28730>