

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:

11/18/2011

SUBJECT:

BIND 9 Resolver crashes after logging an error in query.c

OVERVIEW:

Organizations across the Internet reported crashes interrupting service on BIND 9 nameservers performing recursive queries. Affected servers crashed after logging an error in query.c with the following message: "INSIST(! dns_rdataset_isassociated(sigrdataset))" Multiple versions were reported being affected, including all currently supported release versions of ISC BIND 9. ISC is actively investigating the root cause and has produced patches which prevent the crash. Further information will be made available soon.

SYSTEMS AFFECTED:

BIND 9.4-ESV (all), 9.6-ESV (all), 9.7 (all), 9.8 (all)

RISK:

Large and medium government entities: **High**

Small government entities: **High**

Home users: **High**

DESCRIPTION:

An as-yet unidentified network event caused BIND 9 resolvers to cache an invalid record, subsequent queries for which could crash the resolvers with an assertion failure. ISC is working on determining the ultimate cause by which a record with this particular inconsistency is cached. At this time we are making available a patch which makes named recover gracefully from the inconsistency, preventing the abnormal exit.

The patch has two components. When a client query is handled, the code which processes the response to the client has to ask the cache for the records for the name that is being queried. The first component of the patch prevents the cache from returning the inconsistent data. The second component prevents named from crashing if it detects that it has been given an inconsistent answer of this nature.

RECOMMENDATIONS:

The following actions should be taken:

Upgrade BIND to one of the following patched versions: BIND 9.8.1-P1, 9.7.4-P1, 9.6-ESV-R5-P1, 9.4-ESV-R5-P1.

REFERENCES:

Infoblox:

<http://www.infoblox.com/en/news/press-releases/2011/infoblox-customers-protected-against-recent-dns-vulnerability.html>

Internet Storm Center:

<http://isc.sans.edu/diary.html?storyid=12049>

CVE:

<http://www.isc.org/software/bind/advisories/cve-2011-4313>

