

## **NISCC Vulnerability Advisory 589088/NISCC/DNS**

### **Vulnerability Issue in Implementations of the DNS Protocol**

#### **Version Information**

|                    |                  |
|--------------------|------------------|
| Advisory Reference | 589088/NISCC/DNS |
| Release Date       | 24 May 2005      |
| Last Revision      | 4 Nov 2005       |
| Version Number     | 1.4              |

#### **Acknowledgement**

This issue was identified by Dr. Steve Beaty from the Department of Mathematical and Computer Sciences at the Metropolitan State College of Denver.

#### **What is Affected?**

The vulnerability described in this advisory affect the Domain Name System (DNS) protocol. Many vendors include support for this protocol in their products and may be impacted to varying degrees, if at all.

#### **Impact**

If exploited, this vulnerability could allow an attacker to create a Denial-of-Service condition.

#### **Severity**

The severity of this vulnerability varies by vendor; please see the 'Vendor Information' section below for further information. Alternatively contact your vendor for product specific information.

#### **Summary**

A vulnerability affecting the Domain Name System (DNS) protocol was identified by Dr. Steve Beaty from the Department of Mathematical and Computer Science of Metropolitan State College of Denver.

The Domain Name System (DNS) protocol is an Internet service that translates domain names into Internet Protocol (IP) addresses. Because domain names are alphabetic, they're easier to remember,

however the Internet is really based on IP addresses; hence every time a domain name is requested, a DNS service must translate the name into the corresponding IP address.

The vulnerability concerns the recursion process used by some DNS implementations to decompress compressed DNS messages. Under certain circumstances, it is possible to cause the DNS server to terminate abnormally.

All users of applications that support DNS are recommended to take note of this advisory and carry out any remedial actions suggested by their vendor(s).

## **Details**

Under certain circumstances, it is possible to cause both DNS servers and DNS clients to terminate abnormally by sending it malformed messages.

The text portions of DNS messages are specified by first giving the character count, followed by the characters themselves. For example to specify 'test.test.com', the message would look like '0x04test0x04test0x03com0x00' using 16-bit numbers. From RFC1035, Section 4.1.4 "Message Compression" specifies a way to create smaller messages so that they can easily fit into a DNS UDP packet. Hence if the top two bits of the label length byte are 1, the remaining 14 bits specify an offset from the beginning of the text on where the remaining characters can be found. This way, redundant information can be removed and hence create a smaller message.

Given this type of DNS message, the most obvious method to decode it is by using recursion. However consider a message that contains a code that instructs the DNS process to go to an illegal address once the end of the string is reached; if recursion is used to decode such a message, some DNS implementation may enter into a loop and eventually exhaust the stack. If this happens, then it would be possible for the DNS service to terminate and hence cause a denial-of-service condition.

The following CVE IDs have been allocated for this vulnerability:

- CAN-2005-0036
- CAN-2005-0037
- CAN-2005-0038

Please refer to the 'Vendor Information' section for further details on how the CVE IDs are assigned.

## Mitigation

Patch all affected implementations.

## Solution

Please refer to the 'Vendor Information' section of this advisory for platform specific remediation.

## Vendor Information

The following vendors have provided information about how their products are affected by this vulnerability.

*Please note that [JPCERT/CC](http://jpcert/cc) have released a Japanese language advisory for this vulnerability which contains additional information regarding Japanese vendors. This advisory is available at <http://jvn.jp/niscc/NISCC-589088/index.html>.*

|                           |                         |
|---------------------------|-------------------------|
| <u>Apple Computer Inc</u> | <u>NEC</u>              |
| <u>DeleGate</u>           | <u>pdnsd</u>            |
| <u>DNRD</u>               | <u>pjbdns</u>           |
| <u>Fujitsu</u>            | <u>Posadis</u>          |
| <u>Hitachi Ltd</u>        | <u>PowerDNS</u>         |
| <u>ISC</u>                | <u>SUN Microsystems</u> |
| <u>Juniper Networks</u>   | <u>SuSE</u>             |
| <u>Microsoft</u>          | <u>Wind River</u>       |

### Apple Computer Inc

Mac OS X and Mac OS X Server are not vulnerable to NISCC issue #589088.

### DeleGate

Many buffer overflows, including the one in DNS, in DeleGate for long time was swept out in a bundle at version 8.10.3. Thus upgrading to DeleGate/8.10.3 or later is strongly recommended. See URL: <http://www.delegate.org/delegate/updates/>.

This has been assigned the CVE ID CAN-2005-0036: Denial-of-Service on DeleGate v8.10.2 and prior.

### DNRD

DNRD 2.18 and above is confirmed to be not vulnerable.

All users of version 2.10 are recommended to upgrade to latest

available on <http://dnrd.sourceforge.net>.

This has been assigned the CVE ID CAN-2005-0037: Denial-of-Service on DNRD v2.10.

### Fujitsu

Fujitsu provide the information on this issue:

<http://software.fujitsu.com/jp/security/niscc/niscc.html#589088-DNS>

(only in Japanese)

### Hitachi Ltd

Hitachi products are NOT Vulnerable to this issue.

### ISC

None of the BIND 9 releases or BIND 8 releases (since at least 8.3.7) is vulnerable.

### Juniper Networks

Juniper Networks products are not susceptible to this vulnerability.

### Microsoft

Statement from Microsoft Security Response Centre:

We have conducted an investigation of the issue you had reported. At this point, we have determined that the MS implementation of DNS is not affected.

### NEC

NEC products are NOT susceptible to this vulnerability.

- We continue to check our products.

### pdnsd

Most of the versions of pdnsd published by Thomas Moestl and Paul Rombouts, in particular versions 1.1.7 and later, have been found not to be susceptible to the DNS name compression vulnerability (NISCC Vulnerability #589088). However, versions prior to 1.2 are known to contain a number of unrelated

vulnerabilities. All users of pdnsd are therefore advised to upgrade to version 1.2 or later.

### pjbdns

These packets are no problem for dnscache, tinydns, and clients using the djbdns client library. The underlying dns\_packet\_getname() function deliberately limits itself to 1000 iterations.

### Posadis

All Posadis products, including the Poslib DNS library and the Posadis DNS server, are not, and have never been, vulnerable to this problem.

### PowerDNS

The current version of PowerDNS, 2.9.17, released January 11th of 2005 and before this advisory, is not vulnerable. PowerDNS 2.9.16, released on February 28th of 2004, and earlier versions can temporarily be brought down by a packet with a looping label.

Earlier versions of PowerDNS do contain a check against 'looping labels' but due to a typo this check would not actually prevent loops from crashing the daemon.

Although probably completely accidental, the 2.9.17 release was accompanied by a security warning indicating that a possible cause of denial of service was fixed, the cause exactly being the issue raised by this advisory.

The denial of service is mitigated slightly by the 'guardian' feature of PowerDNS which restarts the server automatically in case of failure or database problems. The PowerDNS recursor does not benefit from this feature when ran in standalone mode, only the authoritative process restarts itself.

On reception of a packet with a looping label, 2.9.17 reports a warning:

On retrieving question of packet from xxx.yyy.zzz.www, encountered error: Looping label when parsing a packet. Version 2.9.17 is widely reported to be a painless upgrade from 2.9.16 with most major PowerDNS deployments already running 2.9.17.

This has been assigned the CVE ID CAN-2005-0038: Denial-of-Service on PowerDNS v2.9.16 and prior.

#### SUN Microsystems

We have investigated the DNS server as well as the DNS client tools shipped with all currently supported releases of Solaris (7, 8, 9, and 10) and have determined that we are not affected by this vulnerability.

#### SuSE

SUSE LINUX does not ship the vulnerable BIND version and is therefore not affected.

#### Wind River

The DNS Client shipped with currently supported versions of the VxWorks Operating System is not vulnerable to this attack. A DNS server does not ship with the VxWorks operating system at this time.

### **Acknowledgements**

The NISCC Vulnerability Team would like to thank Steve Beaty, who identified this vulnerability and reported it to NISCC, and who assisted NISCC in producing the test tool for this issue.

The NISCC Vulnerability Team would also like to thank the vendors for their co-operation in handling this vulnerability and to JPCERT/CC for co-ordinating this issue in Japan.

### **Contact Information**

The NISCC Vulnerability Management Team can be contacted as follows:

|           |   |
|-----------|---|
| Email     | <a href="mailto:vulteam@nisc.gov.uk">vulteam@nisc.gov.uk</a><br><i>(Please quote the advisory reference in the subject line.)</i> |
| Telephone | +44 (0)870 487 0748 Extension 4511<br><i>(Monday to Friday 08:30 - 17:00)</i>   |
| Fax       | +44 (0)870 487 0749   |

|      |  |
|------|--|
| Post | Vulnerability Management Team<br>NISCC<br>PO Box 832<br>London<br>SW1P 1BG |
|------|--|

We encourage those who wish to communicate via email to make use of our PGP key. This is available from <http://www.niscc.gov.uk/niscc/publicKey2-en.pop>.

Please note that UK government protectively marked material should not be sent to the email address above.

If you wish to be added to our email distribution list, please email your request to [uniras@niscc.gov.uk](mailto:uniras@niscc.gov.uk).

### **What is NISCC?**

For further information regarding the UK National Infrastructure Security Co-Ordination Centre, please visit the NISCC web site at: <http://www.niscc.gov.uk/>

Reference to any specific commercial product, process or service by trade name, trademark manufacturer or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by NISCC. The views and opinions of authors expressed within this notice shall not be used for advertising or product endorsement purposes.

Neither shall NISCC accept responsibility for any errors or omissions contained within this advisory. In particular, they shall not be liable for any loss or damage whatsoever, arising from or in connection with the usage of information contained within this notice.

© 2005 Crown Copyright

### **Revision History**

|             |  |
|-------------|--|
| 24 May 2005 | Initial release (1.0)<br>Added NEC's Vendor Statement (1.1)  |
| 25 May 2005 | Added Apple's Vendor Statement<br>Added Hitachi's Vendor Statement<br>Added Fujitsu's Vendor Statement<br>Added SUN's Vendor Statement (1.2) |
| 3 Jun 2005  | Added Wind River's Vendor Statement (1.3)  |
| 4 Nov 2005  | Modified Wind River's Vendor Statement (1.4)   |

<End of NISCC Vulnerability Advisory>