NISCC Vulnerability Advisory 144154/NISCC/DNS

Vulnerability Issues in Implementations of the DNS Protocol

Version Information

Advisory Reference	144154/NISCC/DNS
Release Date	25 April 2006
Last Revision	26 April 2006
Version Number	1.1

Acknowledgement

The DNS Test Tool was created by the Oulu University Secure Programming Group (OUSPG) from the University of Oulu in Finland.

What is Affected?

The vulnerabilities described in this advisory affect implementations of 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, these vulnerabilities could cause a variety of outcomes including, for example, a Denial-of-Service (DoS) condition. In most cases, they can expose memory corruption, stack corruption or other types of fatal error conditions. Some of these conditions may expose the protocol to typical buffer overflow exploits, allowing arbitrary code to execute or the system to be modified.

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

During 2002 the Oulu University Secure Programming Group (OUSPG) discovered a number of implementation specific vulnerabilities in the Simple Network Management Protocol (SNMP). Further work has been done to identify implementation specific

vulnerabilities in related protocols that are used in critical infrastructure. The DNS protocol, which is the primary naming system used on the Internet, was studied as part of this program of work.

DNS is an Internet service that translates domain names into Internet Protocol (IP) addresses and vice versa. Because domain names are alphabetic, they're easier to remember, however the Internet is really based on IP addresses; therefore every time a domain name is requested, a DNS service must translate the name into the corresponding IP address.

OUSPG has developed a PROTOS DNS Test Suite for DNS implementations and employed it to validate their findings against a number of products from different vendors. NISCC has contacted multiple vendors whose products support the DNS protocol and provided them with the test tool to allow them to test their implementations. NISCC believes that most of the relevant vendors who provide support for the DNS protocol have been covered by this advisory.

Details

DNS is a system that stores information associated with domain names in a distributed database on networks such as the Internet. The domain name system associates many types of information with domain names, but most importantly, it provides the IP address associated with the domain name. It also lists mail exchange servers accepting e-mail for each domain and a wide variety of other records.

The OUSPG DNS Test Suite covers a limited set of information security and robustness related implementation errors for the DNS protocol.

The factors behind choosing DNS included:

- DNS is a fundamental infrastructure of the Internet, most Internet applications are dependent on it.

- DNS implementations are ubiquitous: present in servers, end-user equipment such as personal computers or mobile phones and in routers and firewalls. Therefore DNS may be a potential attack vector in a variety of scenarios against a variety of systems and infrastructure components.

- There are no free, publicly available robustness test suites to evaluate DNS implementations.

The material contained in the test suite covers basic queries, dynamic updates, basic responses and zone transfers. However please be aware that the test material does not cover cache poisoning or address spoofing vulnerabilities.

There are three sets of test materials available with the tool; these are specifically designed for the following scenarios:

1. The Query Material -> [queries, dynamic DNS updates] -> DNS server
2. The Response Material -> [query replies] -> DNS server
3. The Response Material -> [query replies] -> DNS stub resolver (client)
4. The Zone Transfer Material -> [zone transfers] -> secondary DNS server

The test material simulates hostile input to the DNS implementation by sending invalid and/or abnormal packets. Therefore by applying the OUSPG DNS Test Suite to a variety of products, several vulnerabilities can be revealed that can have varying effects.

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 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-144154/index.html

Cisco Systems, Inc
Delegate
Ethereal
Hitachi
ISC
Juniper Networks
MyDNS
pdnsd
Sun
Wind River

Microsoft

Cisco Systems, Inc

Cisco Systems is currently testing its DNS related products. We will provide updates if warranted at http://www.cisco.com/go/psirt.

Delegate

Vulnerable:
DeleGate/9.0.5 (DEVELOPMENT) and prior versions
DeleGate/8.11.5 (STABLE) and prior versions
Not Vulnerable:
DeleGate/9.0.6 and subsequent versions
DeleGate/8.11.6 and subsequent versions

DeleGate is an application level gateway (proxy server) which relays multiple application protocols including HTTP, FTP, SMTP, SOCKS, DNS; running on Unix and Windows. There have been bugs in its DNS protocol handling unit where a DNS response message is analyzed.

Due to this problem, DeleGate can suffer a denial-of-service attack.

For some crafted or broken response messages, it reads the message data area beyond the real size of it, or read it in infinitely recursive function call. Then the DeleGate process will abort causing segmentation fault or so accessing non-existent address or non-available memory.

DeleGate as DNS proxy, ICP server and UDP-relay might stop their service receiving such broken DNS response, since the abortion occurs in the main process which is not to be restarted automatically by itself.
Other DeleGate proxies for other protocols do not stop servicing but a child process for a session might abort without returning response message of each application protocol.

These bugs have been fixed in version 9.0.6 (development version) and 8.11.6 (stable version). The impact for resent versions is not more than DoS, but upgrading to these versions (or subsequent ones) is recommended. The impact can be more serious in ancient versions of DeleGate prior to 8.10.3 which also include many other kind of dangers (http://www.delegate.org/mail-lists/delegate-en/2793), so they must be upgraded anyway.

Ethereal

The Ethereal development team is investigating the reported vulnerabilities to determine if any versions of Ethereal are affected.

We will provide updated status information in the near future.

Hitachi

Hitachi believe that the AlaxalA Networks AX series, Hitachi GR2000/GR4000/GS4000/GS3000 and Hitachi HI-UX are NOT vulnerable to this issue.

ISC

ISC has reviewed a bug that can cause named to terminate abnormally if a broken TSIG is present in the second or later message of a zone transfer. However, this is not considered high-risk as the first message must have a correct TSIG present for the transaction to continue. A fix will be included in a future BIND release.

Juniper Networks

The OUSPG PROTOS c09-dns-response test tool was run against all Juniper Networks platforms. JUNOS and ScreenOS were unaffected. Tests against JUNOSe, found on the E-series routers, did result in an issue with the DNS client code (ref: KA 23381). The issue was resolved in the following JUNOSe updates: 5-3-5p0-2, 6-0-3p0-6, 6-0-4, 6-1-3p0-1, 7-0-1p0-7, 7-0-2, 7-1-0p0-1, 7-1-1. Later JUNOSe releases are unaffected.

Microsoft

Microsoft are still testing their products and will provide an update when more information is available.

MyDNS

MyDNS 1.1.0 has been released which contains a fix for a “query-of-death” DoS bug uncovered by the test suite. New versions can be obtained from:
http://mydns.bboy.net/

pdnsd

The current maintainer of the pdnsd project, Paul A. Rombouts, has run tests on pdnsd with the DNS Test Suite mentioned here and discovered one significant flaw in the pdnsd code, which affects several versions of pdnsd. A DNS query with an unsupported QTYPE or QCLASS can cause pdnsd to leak memory. The amount of memory used by pdnsd may thus grow continually and unbounded and may eventually cause pdnsd to crash or cause the system to become sluggish and unresponsive. All users of pdnsd are advised to upgrade to version 1.2.4 or later of pdnsd, which has a fix for this leak and is available at:
http://www.phys.uu.nl/~rombouts/pdnsd.html

Sun

Sun Microsystems is currently investigating the impact of the OUSPG DNS test suite to Sun's products. If any issues are identified, Sun will publish Sun Alerts which will include details of the impact and suggested resolution for those issues.

Wind River

Wind River does not believe that any of the products we provide are currently vulnerable to the issues described in this Vulnerability Notice.

Acknowledgements

The NISCC Vulnerability Management Team would like to thank OUSPG for producing the DNS Test Tool.

The NISCC Vulnerability Management 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	vulteam@niscc.gov.uk *(Please quote the advisory reference in the subject line.)*
Telephone	+44 (0)870 487 0748 Extension 4511 *(Monday to Friday 08:30 - 17:00)*
Fax	+44 (0)870 487 0749
Post	Vulnerability Management Team NISCC PO Box 832 London 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.

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/

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.

Revision History

25 April 2006	Initial release (1.0)
26 April 2006	Added Vendor Statement from Cisco (1.1)

<End of NISCC Vulnerability Advisory>