

[UNIX] Multiple Remote Vulnerabilities in BIND4 and BIND8

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-11/0035.html>

From: support@securiteam.com

Date: 11/14/02

From: support@securiteam.com

To: list@securiteam.com

Date: 14 Nov 2002 16:59:11 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

Beyond Security would like to welcome Tiscali World Online to our service provider team.

For more info on their service offering IP-Secure, please visit http://www.worldonline.co.za/services/work_ip.asp

Multiple Remote Vulnerabilities in BIND4 and BIND8

SUMMARY

ISS X-Force has discovered several serious vulnerabilities in the Berkeley Internet Name Domain Server (BIND). BIND is the most common implementation of the DNS (Domain Name Service) protocol, which is used on the vast majority of DNS servers on the Internet. DNS is a vital Internet protocol that maintains a database of easy-to-remember domain names (host names) and their corresponding numerical IP addresses.

DETAILS

Affected Versions:

BIND SIG Cached RR Overflow Vulnerability

- * BIND 8, versions up to and including 8.3.3-REL
- * BIND 4, versions up to and including 4.9.10-REL

BIND OPT DoS

- * BIND 8, versions 8.3.0 up to and including 8.3.3-REL

BIND SIG Expiry Time DoS

- * BIND 8, versions up to and including 8.3.3-REL

Securiteam: [UNIX] Multiple Remote Vulnerabilities in BIND4 and BIND8

Impact:

The vulnerabilities described in this advisory affect nearly all currently deployed recursive DNS servers on the Internet. The DNS network is considered a critical component of Internet infrastructure. There is no information implying that these exploits are known to the computer underground, and there are no reports of active attacks. If exploits for these vulnerabilities are developed and made public, they may lead to compromise and DoS attacks against vulnerable DNS servers. Since the vulnerability is widespread, an Internet worm may be developed to propagate by exploiting the flaws in BIND. Widespread attacks against the DNS system may lead to general instability and inaccuracy of DNS data.

Technical description:

BIND SIG Cached RR Overflow Vulnerability

A buffer overflow exists in BIND 4 and 8 that may lead to remote compromise of vulnerable DNS servers. An attacker who controls any authoritative DNS server may cause BIND to cache DNS information within its internal database, if recursion is enabled. Recursion is enabled by default unless explicitly disabled via command line options or in the BIND configuration file. Attackers must either create their own name server that is authoritative for any domain, or compromise any other authoritative server with the same criteria. Cached information is retrieved when requested by a DNS client. There is a flaw in the formation of DNS responses containing SIG resource records (RR) that can lead to buffer overflow and execution of arbitrary code.

BIND OPT DoS

Recursive BIND 8 servers can be caused to abruptly terminate due to an assertion failure. A client requesting a DNS lookup on a nonexistent sub-domain of a valid domain name may cause BIND 8 to terminate by attaching an OPT resource record with a large UDP payload size. This DoS may also be triggered for queries on domains whose authoritative DNS servers are unreachable.

BIND SIG Expiry Time DoS

Recursive BIND 8 servers can be caused to abruptly terminate due to a null pointer dereference. An attacker who controls any authoritative name server may cause vulnerable BIND 8 servers to attempt to cache SIG RR elements with invalid expiry times. These are removed from the BIND internal database, but later improperly referenced, leading to a DoS condition.

Workaround:

As a workaround for DNS servers that do not need recursive DNS functionality, it is recommended to disable recursion within the BIND configuration file:

```
BIND 8, named.conf
options {
    recursion no;
};
```

Securiteam: [UNIX] Multiple Remote Vulnerabilities in BIND4 and BIND8

BIND 4, named.boot
options no-recursion

Where disabling recursion is not possible, a temporary workaround exists that may protect perimeter DNS servers from the remote compromise vulnerability. Due to the nature and organization of stack variables, exploitation is much easier if the attack is embedded within TCP DNS traffic. It is unclear at this time if this attack is possible with UDP traffic on certain architectures. The UDP protocol is used for most DNS related queries and responses, except large responses and zone transfers between primary and secondary DNS servers. Therefore, perimeter DNS servers should be protected by filtering TCP port 53. This workaround will block the exploit technique demonstrated by X-Force, but this solution should be examined carefully to determine if it would not affect normal DNS functionality. This workaround is meant as a temporary solution to offer some level of protection before a patch can be applied.

ISC recommends that BIND installations should be upgraded to BIND version 4.9.11, 8.2.7, 8.3.4 or to BIND version 9. BIND 9 was not affected by any of the vulnerabilities described in this advisory. These versions will be available soon. ISC has made security patches available for the affected versions at the following address:

<<http://www.isc.org/products/BIND/bind-security.html>>
<http://www.isc.org/products/BIND/bind-security.html>

ADDITIONAL INFORMATION

The information has been provided by <<mailto:xforce@iss.net>> X-Force.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

-
- **Previous message:** support@securiteam.com: "[NT] Hyperion FTP Server Directory Traversal Vulnerability"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)