

[NEWS] Multiple Vendors' Domain Name System (DNS) Stub Resolvers Vulnerable to Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-06/0126.html>

From: support@securiteam.com

Date: 06/28/02

From: support@securiteam.com

To: list@securiteam.com

Date: Fri, 28 Jun 2002 08:17:58 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

Multiple Vendors' Domain Name System (DNS) Stub Resolvers Vulnerable to Buffer Overflow

SUMMARY

A buffer overflow vulnerability exists in the DNS resolver library used by BSD and ISC BIND. Other systems that use DNS resolver code derived from ISC BIND may also be affected. An attacker who is able to control DNS responses could exploit arbitrary code or cause a denial of service on vulnerable systems.

DETAILS

The Domain Name System (DNS) provides name, address, and other information about Internet Protocol (IP) networks and devices. By issuing queries to and interpreting responses from DNS servers, IP-enabled network operating systems can access DNS information. When an IP network application needs to access or process DNS information, it calls functions in the stub resolver library, which may be part of the underlying network operating system. On BSD-based systems, DNS stub resolver functions are implemented in the system library libc. In ISC BIND, they are implemented in libbind.

Securiteam: [NEWS] Multiple Vendors' Domain Name System (DNS) Stub Resolvers Vulnerable to Buffer Overflow

The DNS resolver libraries on BSD-based systems (libc), ISC BIND (libbind), and possibly other systems that use code derived from ISC BIND contain a buffer overflow vulnerability in the way the resolver handles DNS responses. Quoting from FreeBSD Security Advisory FreeBSD-SA-02:28.resolv:

DNS messages have specific byte alignment requirements, resulting in padding in messages. In a few instances in the resolver code, this padding is not taken into account when computing available buffer space. As a result, the parsing of a DNS message may result in a buffer overrun of up to a few bytes for each record included in the message.

This problem is not limited to DNS servers or to BIND. Any application that makes use of vulnerable function calls in resolver libraries is likely to be affected. Applications that are statically linked must be recompiled using patched resolver libraries.

Impact:

An attacker who is able to control DNS responses could exploit arbitrary code or cause a denial of service on vulnerable systems. The attacker would need to be able to spoof DNS responses or control a DNS server that provides responses to a vulnerable system. Any code executed by the attacker would run with the privileges of the process that called the vulnerable resolver function.

Solution:

Apply a Patch

Apply a patch from your vendor. In the case of statically linked binaries, it is necessary to recompile using the patched version of the DNS stub resolver libraries.

Upgrade

Upgrade your system as specified by your vendor.

Use Local Caching DNS Server

Using a local caching DNS server that reconstructs DNS answers will prevent malicious answers from reaching vulnerable DNS stub resolver libraries. BIND 9 reconstructs answers in this way, with the exception of forwarded UPDATES. BIND 8 does not reconstruct all answers.

Systems Affected

Vendor – Status – Date Updated

AT&T – Unknown – 27-Jun-2002

Computer Associates – Unknown – 27-Jun-2002

FreeBSD – Vulnerable – 27-Jun-2002

Fujitsu – Unknown – 27-Jun-2002

ISC – Vulnerable – 27-Jun-2002

Lucent – Unknown – 27-Jun-2002

Microsoft Corporation – Unknown – 27-Jun-2002

NetBSD – Vulnerable – 27-Jun-2002

NeXT – Unknown – 27-Jun-2002

OpenBSD – Vulnerable – 27-Jun-2002

Securiteam: [NEWS] Multiple Vendors' Domain Name System (DNS) Stub Resolvers Vulnerable to Buffer Overflow

Wind River Systems – Unknown – 26-Jun-2002

ADDITIONAL INFORMATION

References:

<<http://www.pine.nl/advisories/pine-cert-20020601.asc>>

<http://www.pine.nl/advisories/pine-cert-20020601.asc>

<<ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-02:28.resolv.asc>>

<ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-02:28.resolv.asc>

The information has been provided by <<mailto:joost@pine.nl>> Joost Pol and CERT.

=====

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] Unchecked Buffer in Profile Service Could Allow Code Execution in Commerce Server"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)