

[NEWS] ISC DHCPD Minires Library Contains Multiple Buffer Overflows

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-01/0049.html>

From: support@securiteam.com

Date: 01/18/03

From: support@securiteam.com

To: list@securiteam.com

Date: 19 Jan 2003 00:29:35 +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

ISC DHCPD Minires Library Contains Multiple Buffer Overflows

SUMMARY

The Internet Software Consortium (ISC) has discovered several buffer overflow vulnerabilities in their implementation of DHCP (ISC DHCPD). These vulnerabilities may allow remote attackers to execute arbitrary code on affected systems. At this time, we are not aware of any exploits.

DETAILS

Immune systems:

- * Apple Computer Inc.
- * Cisco Systems Inc.
- * Cray Inc.
- * Fujitsu
- * Hewlett-Packard Company
- * Hitachi
- * IBM
- * Microsoft Corporation
- * MontaVista Software
- * NEC Corporation
- * NetBSD
- * NetScreen

Securiteam: [NEWS] ISC DHCPD Minires Library Contains Multiple Buffer Overflows

- * OpenBSD
- * Openwall GNU/*/Linux
- * Riverstone Networks
- * Sun Microsystems Inc.

Vulnerable systems:

- * BSDI – Vulnerable – 15-Jan-2003
- * ISC – Vulnerable – 15-Jan-2003
- * Red Hat Inc. Vulnerable 15-Jan-2003
- * SuSE Inc. Vulnerable 15-Jan-2003

There are multiple remote buffer overflow vulnerabilities in the ISC implementation of DHCP. As described in RFC 2131, "the Dynamic Host Configuration Protocol (DHCP) provides a framework for passing configuration information to hosts on a TCP/IP network." In addition to supplying hosts with network configuration data, ISC DHCPD allows the DHCP server to dynamically update a DNS server, obviating the need for manual updates to the name server configuration. Support for dynamic DNS updates is provided by the NSUPDATE feature.

During an internal source code audit, developers from the ISC discovered several vulnerabilities in the error handling routines of the minires library, which is used by NSUPDATE to resolve hostnames. These vulnerabilities are stack-based buffer overflows that may be exploitable by sending a DHCP message containing a large hostname value. Note: Although the minires library is derived from the BIND 8 resolver library, these vulnerabilities do not affect any current versions of BIND.

Impact:

Remote attackers may be able to execute arbitrary code with the privileges of the user running ISC DHCPD.

Solution:

Upgrade or apply a patch

The ISC has addressed these vulnerabilities in versions 3.0pl2 and 3.0.1RC11 of ISC DHCPD. If your software vendor supplies ISC DHCPD as part of an operating system distribution, please see the vendor section of this document.

Disable dynamic DNS updates (NSUPDATE)

As an interim measure, the ISC recommends disabling the NSUPDATE feature on affected DHCP servers.

Block external access to DHCP server ports

As an interim measure, it is possible to limit exposure to these vulnerabilities by restricting external access to affected DHCP servers on the following ports:

```
bootps 67/tcp # Bootstrap Protocol Server
bootps 67/udp # Bootstrap Protocol Server
bootpc 68/tcp # Bootstrap Protocol Client
```

Securiteam: [NEWS] ISC DHCPD Minires Library Contains Multiple Buffer Overflows

bootpc 68/udp # Bootstrap Protocol Client

Disable the DHCP service

As a general rule, the CERT/CC recommends disabling any service or capability that is not explicitly required. Depending on your network configuration, you may not need to use DHCP.

ADDITIONAL INFORMATION

The information has been provided by <mailto:cert-advisory@cert.org> CERT Advisory.

=====

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](mailto:cert-advisory@cert.org)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto:cert-advisory@cert.org)

=====

=====

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.