

CERT Advisory CA-2002-12 Format String Vulnerability in ISC DHCPD

Source: <http://www.derkeiler.com/Mailing-Lists/Cert/2002-05/0004.html>

From: CERT Advisory (cert-advisory@cert.org)

Date: 05/08/02

Date: Wed, 8 May 2002 13:27:21 -0400 (EDT)
From: CERT Advisory <cert-advisory@cert.org>
To: cert-advisory@cert.org

-----BEGIN PGP SIGNED MESSAGE-----

CERT Advisory CA-2002-12 Format String Vulnerability in ISC DHCPD

Original release date: May 8, 2002

Last revised:--

Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

- * ISC DHCPD 3.0 to 3.0.1rc8 inclusive

Overview

The Internet Software Consortium (ISC) provides a Dynamic Host Configuration Protocol Daemon (DHCPD), which is a server that is used to allocate network addresses and assign configuration parameters to hosts. A format string vulnerability may permit a remote attacker to execute code with the privileges of the DHCPD (typically root). We have not seen active scanning or exploitation of this vulnerability.

I. Description

ISC's DHCPD listens for requests from client machines connecting to the network. Versions 3 to 3.0.1rc8 (inclusive) of DHCPD contains an option (NSUPDATE) that is enabled by default. NSUPDATE allows the DHCP server to send information about the host to the DNS server after processing a DHCP request. The DNS server responds by sending an acknowledgement message back to the DHCP server that may contain user-supplied data (like a host name). When the DHCP server receives the acknowledgement message from the DNS server, it logs the transaction.

Cert: CERT Advisory CA–2002–12 Format String Vulnerability in ISC DHCPD

A format string vulnerability exists in ISC's DHCPD code that logs the transaction. This vulnerability may permit a remote attacker to execute code with the privileges of the DHCP daemon.

II. Impact

A remote attacker may be able to execute code with the privileges of the DHCPD (typically root).

III. Solution

Note that some of the mitigation steps recommended below may have significant impact on your normal network operations. Ensure that any changes made based on the following recommendations will not unacceptably affect any of your operations.

Apply a patch from your vendor

Appendix A contains information provided by vendors for this advisory.

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.

Ingress filtering

As a temporary measure, it may be possible to limit the scope of this vulnerability by blocking access to DHCP services at the network perimeter.

Ingress filtering manages the flow of traffic as it enters a network under your administrative control. In the network usage policy of many sites, there are few reasons for external hosts to initiate inbound traffic to machines that provide no public services. Thus, ingress filtering should be performed at the border to prohibit externally initiated inbound traffic to non–authorized services. For DHCP, ingress filtering of the following ports can prevent attackers outside of your network from reaching vulnerable devices in the local network that are not explicitly authorized to provide public DHCP services.

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

Appendix A. – Vendor Information

This appendix contains information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will

Cert: CERT Advisory CA-2002-12 Format String Vulnerability in ISC DHCPD

update this section and note the changes in our revision history. If a particular vendor is not listed below, please check the Vulnerability Note (VU#854315) or contact your vendor directly.

Alcatel

The security of our customers' networks is of highest priority for Alcatel. Alcatel is aware of this security issue in the DHCP implementation of ISC and has put measures in place to assess which of its products might be affected and to apply the necessary fixes where required. An update will be shortly published to provide more details on any affected products.

Conectiva

Conectiva Linux 8 ships dhcp-3.0 and is vulnerable to this problem. Updates will be available at our ftp site and an announcement will be sent to our mailing lists as soon as CERT publishes its advisory.

F5 Networks, Inc.

F5 Networks' products do not include any affected version of ISC's DHCPD, and are therefore not vulnerable.

FreeBSD

The FreeBSD base system does not ship with the ISC dhcpd server by default and is not affected by this vulnerability. The ISC dhcpd server is available in the FreeBSD Ports Collection; updates to the ISC dhcp port (ports/net/isc-dhcp3) are in progress and corrected packages will be available in the near future.

IBM

IBM's AIX operating system, all versions, is not vulnerable.

Internet Software Consortium

A patch is included below, and we have a patched version of 3.0 available (3.0p11) and a new release candidate for the next bug-fix release (3.0.1RC9). Both of these new releases are not vulnerable.

```
--- common/print.c Tue Apr 9 13:41:17 2002
+++ common/print.c.patched Tue Apr 9 13:41:56 2002
@@ -1366,8 +1366,8 @@
     *s++ = '.';
     *s++ = 0;
     if (errorp)
- log_error (obuf);
+ log_error ("%s",obuf);
```

Cert: CERT Advisory CA-2002-12 Format String Vulnerability in ISC DHCPD

```
else
- log_info (obuf);
+ log_info ("%s",obuf);
}
#endif /* NSUPDATE */
```

Lotus Development Corporation

This issue does not affect Lotus products.

Microsoft Corporation

Microsoft does not ship the ISC DHCPD program.

NetBSD

NetBSD fixed this during a format string sweep performed on 11-Oct-2000. No released version of NetBSD is vulnerable to this issue.

Silicon Graphics, Inc.

SGI is not vulnerable.

The CERT Coordination Center acknowledges Next Generation Security Technologies as the discoverer of this vulnerability and thanks them and the Internet Software Consortium (ISC) for their cooperation, reporting, and analysis of this vulnerability.

Feedback can be directed to the author: Ian A. Finlay

This document is available from:
<http://www.cert.org/advisories/CA-2002-12.html>

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:
CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

Cert: CERT Advisory CA-2002-12 Format String Vulnerability in ISC DHCPD

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from

http://www.cert.org/CERT_PGP.key

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site

<http://www.cert.org/>

To subscribe to the CERT mailing list for advisories and bulletins, send email to majordomo@cert.org. Please include in the body of your message

subscribe cert-advisory

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

NO WARRANTY

Any material furnished by Carnegie Mellon University and the Software Engineering Institute is furnished on an "as is" basis. Carnegie Mellon University makes no warranties of any kind, either expressed or implied as to any matter including, but not limited to, warranty of fitness for a particular purpose or merchantability, exclusivity or results obtained from use of the material. Carnegie Mellon University does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

Conditions for use, disclaimers, and sponsorship information

Copyright 2002 Carnegie Mellon University.

Revision History

May 8, 2002: Initial release

-----BEGIN PGP SIGNATURE-----

Version: PGP 6.5.8

Cert: CERT Advisory CA-2002-12 Format String Vulnerability in ISC DHCPD

iQCVAwUBPNle2qCVPMXQI2HJAQEJ5gP/SKXwgQG1Z4Y+dQmAqGnHxYEUZuKaPDuLB
zLmkVcPQrpd08DVDNpy3uMK1Mfro3RFLMg5mTON4noHiiIQb5M7iZPWXXV5qnQnt3
s4ga8RseymwUvbNbdBo6x9EdjrM2+iQsrJHbVF0RXXrvZT9zRAg+sfzHtGwEeHxQ3
XuLLU2DySLc=
=Kvhw
-----END PGP SIGNATURE-----

- **Previous message:** [CERT Advisory: "CERT Advisory CA-2002-11 Heap Overflow in Cachefs Daemon \(cachefs\)"](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)