

[UNIX] Multiple Vulnerabilities in Solaris in.rarpd

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-05/0095.html>

From: support@securiteam.com

Date: 05/23/02

From: support@securiteam.com

To: list@securiteam.com

Date: Thu, 23 May 2002 08:48:19 +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 Vulnerabilities in Solaris in.rarpd

SUMMARY

Rarpd is a reverse ARP protocol for small to medium sized networks. In the Solaris implementation (in.rarpd) there seems to be 3 remotely exploitable buffer overflows, 2 locally exploitable and 2 cases of format string exploitability.

DETAILS

Vulnerable code:

In the functions error and syserr there contains 2 common syslog calls without format strings.

```
static void
syserr(s)
char *s;
{
    char buf[256];

    (void) sprintf(buf, "%s: %s", s, strerror(errno));
    (void) fprintf(stderr, "%s: %s\n", cmdname, buf);
    syslog(LOG_ERR, buf);
    exit(1);
}
```

Securiteam: [UNIX] Multiple Vulnerabilities in Solaris in.rarpd

```
/* VARARGS1 */
static void
error(char *fmt, ...)
{
    char buf[256];
    va_list ap;

    va_start(ap, fmt);
    (void) vsprintf(buf, fmt, ap);
    va_end(ap);
    (void) fprintf(stderr, "%s: %s\n", cmdname, buf);
    syslog(LOG_ERR, buf);
    exit(1);
}
```

There are two vulnerable calls that could be exploited locally or remotely.

Vendor status:
Vendor has not been contacted yet.

ADDITIONAL INFORMATION

The information has been provided by <mailto:davidreign@hotmail.com>
david evlis reign.

=====

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] Authentication Flaw in Windows Debugger can lead to Elevated Privileges"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)