

[UNIX] Linux nfs-utils xlog() Off-by-One Bug

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-07/0068.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 07/17/03

To: list@securiteam.com

Date: 17 Jul 2003 13:40:28 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.secureteam.com>

-- promotion

Beyond Security in Canada

Toronto-based Sunrays Technologies is now Beyond Security's representative in Canada.

We welcome ISPs, system integrators and IT systems resellers

to promote the most advanced vulnerability assessment solutions today.

Contact us at 416-482-0038 or at canadasales@beyondsecurity.com

Linux nfs-utils xlog() Off-by-One Bug

SUMMARY

<<http://sourceforge.net/projects/nfs/>> Linux NFS utils package contains remotely exploitable off-by-one bug. A local or remote attacker could exploit this vulnerability by sending a specially crafted request to rpc.mountd daemon.

DETAILS

Vulnerable systems:

- * nfs-utils version 1.0.3 and prior

Immune systems:

- * nfs-utils version 1.0.4 and above

An off-by-one bug exist in xlog() function which handles logging of requests. An overflow occurs when function is trying to add missing trailing new line character to logged string.

Due to miscalculation, if a string passed to the functions is equal or

Securiteam: [UNIX] Linux nfs-utils xlog() Off-by-One Bug

longer than 1023 bytes, the '\0' byte will be written beyond the buffer:

-----8<-----cut-here-----8<-----

```
char buff[1024];
...

va_start(args, fmt);
vsnprintf(buff, sizeof (buff), fmt, args);
va_end(args);
buff[sizeof (buff) - 1] = 0;

if ((n = strlen(buff)) > 0 && buff[n-1] != '\n') {
    buff[n++] = '\n'; buff[n++] = '\0';
}
```

-----8<-----cut-here-----8<-----

Impact:

Local or remote attacker that is capable of sending an RPC request to a vulnerable mount daemon could execute arbitrary code or cause denial of service.

Vendor status:

Vendor has been notified on June 10, 2003. The fix is incorporated in recent 1.0.4 release of nfs-utils.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:funkysh@isec.pl>> Janusz Niewiadomski.

=====

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.