

[UNIX] QNX DHCP Client Privilege Escalation

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-12/msg00090.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 26 Dec 2005 18:40:32 +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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.
<http://www.securiteam.com/maillinglist.html>

QNX DHCP Client Privilege Escalation

SUMMARY

<<http://www.qnx.com/>> QNX is "a commercial POSIX-compliant Unix-like real-time operating system, aimed primarily at the embedded systems market".

A vulnerability in the QNX system allows local users to can change NIC configuration without requiring root privileges.

DETAILS

Vulnerable Systems:
* QNX version 4.25

The dhcp.client program shipped with QNX 4.25 is setuid root.

This obviously enables a normal user to control the NIC's configuration and produce some other attacks such as if the system has some services which depend on 'host/ip based' authentication, for example: NFS, NIS, rlogin, etc.

Some screenshots of QNX running under VMWare are available at:

[UNIX] QNX DHCP Client Privilege Escalation

<http://lms.ispgaya.pt/goodies/qnx/> <http://lms.ispgaya.pt/goodies/qnx/>

ADDITIONAL INFORMATION

The information has been provided by <mailto:lms@xxxxxxxx> Lu s Miguel Ferreira da Silva.

=====

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@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====

=====

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.



- Prev by Date: [*\[NT\] dtSearch DUNZIP32.dll Buffer Overflow*](#)
- Next by Date: [*\[EXPL\] Microsoft IIS Malformed URI DoS \(Exploit\)*](#)
- Previous by thread: [*\[NT\] dtSearch DUNZIP32.dll Buffer Overflow*](#)
- Next by thread: [*\[EXPL\] Microsoft IIS Malformed URI DoS \(Exploit\)*](#)
- Index(es):
 - ◆ [*Date*](#)
 - ◆ [*Thread*](#)