

[NEWS] NetGear RP114 Flooding DoS

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-12/msg00037.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 13 Dec 2005 17:18:43 +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>

NetGear RP114 Flooding DoS

SUMMARY

" <<http://kbserver.netgear.com/products/RP114.asp>> NetGear RP114 is a Cable or DSL Router".

By TCP SYN flooding the NetGear RP114 product, remote attackers can cause the route to deny any incoming communication to the device.

DETAILS

Vulnerable Systems:
* NetGear RP114

By starting a transit TCP SYN flooding the routing between the internal and the external interface is not possible anymore. An attacker can use this to prevent legitimate users from accessing connected networks (e.g. the WAN/Internet). Other devices by NetGear (e.g. routers and wlan access points) may be also affected.

Running TCP SYN flooding is very simple and can be realized by a large variety of public attack tools. But it is also possible to initialize such an attack by misusing a port scanning utility. Starting a scan with nmap

[NEWS] NetGear RP114 Flooding DoS

by Fyodor with the following command is able to reproduce the denial of service:

```
nmap -PS80 192.168.0.0/24
```

It does not matter how many target ports or hosts are defined. It is just important to open approx. more than 740 persistent and half-open connections. It is also required to scan something on the other interface of the device than the attacker is connected to (e.g. scanning an external host by sitting on the internal interface and vice versa).

After a successful attack no further routing between the networks is possible anymore. This makes it impossible for legitimate users to connect to the Internet or another network segment. During this time direct connections to the affected device remains possible (e.g. connection to the web interface or ping).

Workarounds:

1. A reboot of the device can restore the productive status immediately.
2. Waiting for approximately 2 minutes for the device to flush all half-open connections and return to full operational status.

Vendor Status:

No response from NetGear came back. Due the fact the affected device RP114 is not listed on the web site anymore and the last firmware is dated back to 2002, no firmware update could be expected.

Disclosure Timeline:

11/23/05 Marc Ruef verifies the for a long time suspected flaw
11/24/05 Inform the vendor by sending an email to
pressrelations-at-netgear.com
12/12/05 Public advisory

ADDITIONAL INFORMATION

The information has been provided by <<mailto:maru@xxxxxxx>> Marc Ruef.

=====

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@xxxxxxxxxxxxxx

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

=====

=====

[NEWS] NetGear RP114 Flooding DoS

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: [*\[UNIX\] SCO Unixware Setuid 'uidadmin' Scheme Buffer Overflow*](#)
- Next by Date: [*\[NEWS\] Gecko InstallVersion.compareTo Code Execution \(Exploit\)*](#)
- Previous by thread: [*\[UNIX\] SCO Unixware Setuid 'uidadmin' Scheme Buffer Overflow*](#)
- Next by thread: [*\[NEWS\] Gecko InstallVersion.compareTo Code Execution \(Exploit\)*](#)
- Index(es):
 - ◆ [*Date*](#)
 - ◆ [*Thread*](#)