

[VulnWatch] 3Com OfficeConnect Remote 812 ADSL router exposes internal LAN computer's ports during outbound and inbound TCP and UDP sessions

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2003-04/0001.html>

From: Michael Puchol (mpuchol@sonar-security.com)
Date: 04/01/03

From: "Michael Puchol" <mpuchol@sonar-security.com>
To: "Bugtraq" <bugtraq@securityfocus.com>, "C2 Security" <security-submit@C2Security.org>, "Packe
Date: Tue, 1 Apr 2003 01:25:13 +0200

3Com OfficeConnect Remote 812 ADSL router exposes internal LAN computer's ports during outbound and inbound TCP and UDP sessions.

Overview:
=====

The 3Com 812 is a widely-deployed router, found in many ISPs ADSL lines. The router allows basic packet filtering and has two security settings for protecting file and printer shares and mitigating DoS attacks, together with two modes of operation, single-workstation, where all inbound traffic is routed to a single, configurable internal IP address, and NAT mode, where inbound packets destined to specific ports can be routed to specific internal IP addresses, by means of a TCP & UDP port mapping table, or dropped altogether. This second mode of operation gives one layer of protection to internal computers, for example, by denying access to their NetBIOS ports unless specifically mapped in the NAT table. It also allows many computers to share a single ADSL line by providing a default gateway for internet access.

This theoretical protection against inbound malicious traffic is fatally flawed in the tested product, as soon as one of the internal computers connects to an external computer, or an external computer connects to a service running in one of the internal computers, as the router will then forward all inbound packets to the internal IP address which initiated or received the connection.

Tested product:
=====

3Com OfficeConnect Remote 812 ADSL Router, product code 3CR414492. A router with internal firmware V1.17 has been found vulnerable, V1.19 is to be

tested, but in the firmware upgrade description this problem is not mentioned as being fixed or otherwise.

Description:

=====

To better picture the scenario, a step-by-step description of example processes are provided:

a) Internally-initiated connection:

1. The internal computer (A) connects to an external computer's (B) HTTP server on port 80.
2. Computer (B) serves the web page, and now has access to all open ports on computer (A).

b) Externally-initiated connection:

1. The internal computer (A) is running an FTP server, on default port 21. Port 21 of the WAN interface is mapped in the NAT table of the 3Com router towards computer (A)'s LAN IP, port 21.
2. An external client (B) starts a TCP session to computer (A) on port 21.
3. All locally open ports on computer (A) are now available for access to computer (B).

This means that, for example, a user could be instantly attacked by simply accessing a remote web server, with means that could even be automated. No exploit code for this automated attack has been developed by us, since this flaw could result in many attack scenarios, such as planting an attack bot, zombie, ftp server, or remote-control software, to NetBIOS port spam messaging, etc.

The router opens all inbound ports when an outbound connection occurs to ANY port on the remote computer, it is not limited to http or other common ports. For example, software installed on the internal computers which periodically checks for updates in a remote server on 'odd' ports will render the computer performing the checks vulnerable to attacks from the remote server's IP address.

Both internally and externally-initiated connections will cause the router to open all ports, which represents a very serious security hazard, as for example, a web server's NetBIOS ports could be exposed to all it's visitors. The implications to organisations using this router are very serious.

The effect takes place with TCP and UDP traffic, so an outbound UDP packet will also cause all packets sent back from the destination IP to any port on the originating machine to pass through the router unimpeded. ICMP packets don't cause the router to open the ports for inbound traffic.

Once the connection has ended, the router will keep all the ports open for between 2 and 3 minutes, time during which it is still possible to access

the internal computer's ports from the WAN side.

Possible solutions:

=====

Run a firewall and IDS between the router and the internal network, which properly filters all traffic coming from the router. It is then possible to eliminate external connection attempts to particular ports, which is what the router should be doing in the first place. Mapping vulnerable ports to internal, non-existent or protected IP addresses as fixed NAT routes has no effect on this problem, as an internal computer's ports will still be exposed by the router when a connection occurs between it and an external computer.

Reproducing the problem:

=====

Interested parties can follow this procedure to reproduce the vulnerability:

a) Internally-initiated connection, TCP protocol:

1. Configure the affected 3Com router in NAT mode, mapping ports in the NAT table is not required.
2. Setup a listening netcat[1] on the computer (A) behind the 3Com router, for example 'nc -l -p 36000 -t -e cmd.exe' will launch a command shell when another computer connects to this computer's port 36000 TCP.
3. Start a TCP session towards another computer (B), for example, an FTP session.
4. From (B), telnet to (A) on port 36000.
5. You will see a command prompt from (A) in the telnet client, from which you could issue commands that will execute in (A).

b) Internally-initiated connection, UDP protocol:

1. Repeat steps 1 and 2 in a).
2. Using a TFTP client, for example, send a file download request to (B). There is no need to have a TFTP server running in (B) for the vulnerability to occur, or to send any actual UDP data back to (A).
3. From (B), telnet to (A) on port 36000.
4. You will see a command prompt from (A) in the telnet client.

c) Externally-initiated connection, TCP protocol:

1. Setup a service in computer (A), for example, a web server on port 80.
2. Map port 80 in the 3Com router's NAT table to (A)'s LAN IP address.
3. Setup a listening netcat as per step 2 in a).
4. Start, from computer (B) a TCP session to port 80 directed to the 3Com's WAN IP. This will then be routed to (A) by the 3Com, as any other legitimate http transaction.
5. From (B), telnet to (A) on the port netcat is listening to.

6. You will see a command prompt from (A) in the telnet client.

Vendor status:

=====

3Com's webmaster was notified on the 28th of March 2003 via email, and given 2 working days to provide a valid security contact within 3Com (since no security or similar contact information is available at 3Com's website), with which an exchange of information about this vulnerability can take place. If such contact had taken place, 7 days would have been given before posting this vulnerability report for an initial assesment. A longer waiting period would have been considered if warranted by the particular nature of the vulnerability, for example, to allow the manufacturer to provide a fix or updated firmware. Since no further contact, apart from an initial email from 3Com's webmaster stating that 3Com does not provide internal contact information, has taken place, we have decided to release this report.

References:

=====

[1] Netcat, the network swiss army knife, can be found at

http://www.atstake.com/research/tools/network_utilities/

[2] 3Com's product site for this router,

http://www.3com.com/products/en_US/detail.jsp?tab=support&pathtype=support&sku=3CR414492-US

Acknowledgements:

=====

Special thanks go to Jerry Shenk (jas@decommunications.com), whose extensive help in testing this vulnerability was vital to it's confirmation.

Michael Puchol

Sonar Security

mpuchol@sonar-security.com

<http://www.sonar-security.com>