

[VulnWatch] 3com NBX IP Phone Call manager Denial of Service – Update

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2003-04/0049.html>

From: Michael Scheidell (*scheidell_at_secnap.net*)

Date: 04/27/03

To: bugtraq@securityfocus.com

Date: Sat, 26 Apr 2003 21:37:43 -0400 (EDT)

Revision Date: April 25, 2003

Reason for Revision: 3com updated nbx firmware to 4_1_21, Add bugtraq-id

Systems: 3com NBX IP Phone Call manager, FW Versions through 4_1_21

Severity: Critical

Category: Denial of Service

Classification: Boundary Condition Error

BugTraq-ID: 6297

CERT VU#:[VU#317417]

Vendor URL: www.3com.com, www.windriver.com

Author: Michael S. Scheidell, SECNAP Network Security

Original Release date: December 2nd, 2002

Notifications: (3com, WindRiver and CERT) Notified October 31st, 2002

Last contact with 3com: November 22nd, 2002

Attempted contact with 3com: April 15th, 2003

Last contact with WindRiver: December 6rd, 2002

Discussion: (From 3com's and WindRiver's web site)

3Com® SuperStack® 3 NBX® and 3Com NBX 100 networked telephony solutions offer wide-ranging price/performance alternatives to fit your business needs today and tomorrow. 3Com® SuperStack® 3 NBX® Networked Telephony Solution Delivers robust, full-featured business communications for up to 1500 devices (lines/stations) Ensures high system availability with the Wind River VxWorks real-time operating system (also used in pacemakers and artificial hearts), so server and PC downtime does not impact your telephone service.

VxWorks and pSOSystem are the most widely adopted real-time operating systems (RTOSs) in the embedded industry — for good reason. They are flexible, scalable, reliable, and available on all popular CPU platforms. They are also, by most measures, the fastest RTOSs available today.

Exploit: It was possible to make the remote FTP server crash by issuing this command :

VulnWatch: [VulnWatch] 3com NBX IP Phone Call manager Denial of Service – Update

CEL aaaa[...]aaaa where string is 2048 bytes long. This can be done with netcat, a windows client by telnetting to the nbx server on port 21 or by running the vxworks_ftpd.nasl test in nessus (www.nessus.org)

The 3com NBX uses VXWORKS Embedded Real time Operating system and what appears to be their own internal ftp server. This buffer overflow problem seems to be one similar to the AIX ftpd reported in CVE 1999-0789 and has been assigned bugtraq id 6297

By sending a specific string of data to the ftp server, an attacker can not only disable the ftp server, but the integrated web based administrative console and the call manager preventing diagnostics, control and all incoming, outgoing or internal calls. Any calls in progress cannot be disconnected, and in the case of long distance calls, could result in excessiv