

[VulnWatch] iDEFENSE Security Advisory 10.02.2002: Net-SNMP DoS Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2002-10/0008.html>

From: David Endler (dendler@idefense.com)

Date: 10/02/02

From: "David Endler" <dendler@idefense.com>

To: vulnwatch@vulnwatch.org

Date: Wed, 2 Oct 2002 16:14:45 -0400

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

iDEFENSE Security Advisory 10.02.2002: Net-SNMP DoS Vulnerability
20:00 GMT, October 2, 2002

I. BACKGROUND

The Net-SNMP package, formerly known as ucd-snmp, is a suite of tools relating to the Simple Network Management Protocol (SNMP). It includes an extensible agent, an SNMP daemon, tools to request or set information from SNMP agents, tools to generate and handle SNMP traps, a version of the Unix 'netstat' command using SNMP, and a graphical Perl/Tk/SNMP based mib browser. More information about the package is available at <http://net-snmp.sourceforge.net>.

II. DESCRIPTION

The SNMP daemon included in the Net-SNMP package can be crashed if it attempts to process a specially crafted packet. Exploitation requires foreknowledge of a known SNMP community string (either read or read/write). This issue potentially affects any Net-SNMP installation in which the "public" read-only community string has not been changed.

III. ANALYSIS

By sending the SNMP daemon a packet without having first setup a session, a vulnerability in the following segment of code from agent/snmp_agent.c, handle_var_requests(), line 1,876, can be exploited:

```
for (i = 0; i <= asp->treecache_num; i++) {  
    reginfo = asp->treecache[i].subtree->reginfo;
```

```
status = netsnmp_call_handlers(reginfo, asp->reqinfo,  
asp->treecache[i].requests_begin);
```

Despite the fact that “asp->treecache_num” is NULL, the “<=” comparison in the for() loop allows entry into the block. At this point, the SNMP daemon attempts to de-reference a NULL pointer leading to a SIGSEGV. Since the SNMP daemon must parse the attack packet, an attacker must pass the appropriate ACL (public/read is sufficient).

IV. DETECTION

Net-SNMP 5.0.1, 5.0.3 and 5.0.4.pre2 are vulnerable.

V. WORKAROUND/RECOVERY

Restart the affected SNMP daemon to restore normal functionality.

VI. VENDOR FIX/RESPONSE

Net-SNMP 5.0.5 has been released which fixes the described vulnerability. It is available at http://sourceforge.net/project/showfiles.php?group_id=12694.

VII. CVE INFORMATION

The Mitre Corp.'s Common Vulnerabilities and Exposures (CVE) Project has assigned the identification number CAN-2002-1170 to this issue.

VIII. DISCLOSURE TIMELINE

9/01/2002 Issue disclosed to iDEFENSE
9/24/2002 Maintainer of Net-SNMP notified at <http://net-snmp.sourceforge.net/>
9/24/2002 iDEFENSE clients notified
9/27/2002 Response received from Wes Hardaker, hardaker@users.sourceforge.net
10/1/2002 Vendor fix made available
10/2/2002 Issue disclosed to public

IX. CREDIT

Andrew Griffiths (andrewg@d2.net.au) disclosed this vulnerability to iDEFENSE

Get paid for security research
<http://www.idefense.com/contributor.html>

Subscribe to iDEFENSE Advisories:
send email to listserv@idefense.com, subject line: "subscribe"

About iDEFENSE:

iDEFENSE is a global security intelligence company that proactively monitors sources throughout the world — from technical vulnerabilities and hacker profiling to the spread of viruses and other malicious code. iALERT, our security intelligence service, provides decision-makers, frontline security professionals and network administrators with timely access to actionable intelligence and decision support on cyber-related threats. For more information, visit <http://www.idefense.com>.

--dave

David Endler, CISSP
Director, Technical Intelligence
iDEFENSE, Inc.
14151 Newbrook Drive
Suite 100
Chantilly, VA 20151
voice: 703-344-2632
fax: 703-961-1071

dendler@idefense.com
www.idefense.com

-----BEGIN PGP SIGNATURE-----

Version: PGP 7.1.2

Comment: <http://pgp.mit.edu:11371/pks/lookup?op=getA>

iQA/AwUBPZtS9UrdNYRLCswqEQJZTACeKzigVrxMMBk6Z8Dhqn+fviL+udcAnAvy
0bBhknYmnBIFkrBgoepH52KQ
=4m8X

-----END PGP SIGNATURE-----

-
- **Previous message:** [Matt Moore: "\[VulnWatch\] wp-02-0012: Carello 1.3 Remote File Execution \(Updated 1/10/2002\)"](#)
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)