security-assessment.com

Vulnerability Advisory

Name	Asterisk - chan_skinny Remote Unauthenticated Heap Overflow
Vendor Website	http://www.asterisk.org
Date Released	October 18, 2006
Affected Software	Asterisk 1.0.x, 1.2.x
Researcher	Adam Boileau adam.boileau@security-assessment.com

Description

Asterisk is "The Opensource PBX", a popular software telephony server.

The Asterisk Skinny channel driver for Cisco SCCP phones (chan_skinny.so) incorrectly validates a length value in the packet header. An integer wrap-around leads to heap overwrite, and arbitrary remote code execution as root.

Details

The function 'static int get_input(struct skinnysession *s)' in chan_skinny.c incorrectly validates a user supplied length in the packet header. In the code below, four bytes of data are read from the socket, cast to a signed integer, and assigned to dlen. If dlen is between -1 and -8 then (dlen + 8) will integer wrap to be greater than zero, but less than sizeof(s->inbuf) for the purposes of this comparison.

Next, dlen + 4 is passed to read() as the maximum number of bytes to write to s->inbuf+4. Read() takes an unsigned value, so dlen is interpreted as a very large number. For example, a value of -6 is interpreted as 0xfffffffa bytes. This instructs read() to write beyond the allocated 1000 byte length of the buffer s->inbuf.

Code asterisk-1.2.12.1/channels/chan_skinny.c lines 2860-2870

```
res = read(s->fd, s->inbuf, 4);     // <- integer read from attacker
if (res != 4) {
     ast_log(LOG_WARNING, "Skinny Client sent less data than expected.\n");
     return -1;
}
dlen = letohl(*(int *)s->inbuf);   // <- input 0xfffffffa interpreted as signed
if (dlen+8 > sizeof(s->inbuf)) {   // <- integer wrap to +2 bypasses this check
     dlen = sizeof(s->inbuf) - 8;
}
*(int *)s->inbuf = htolel(dlen);        // Some casting just for amusement
res = read(s->fd, s->inbuf+4, dlen+4);  /* <- dlen now unsigned again
                                         *  permitting read() to write up to
                                         * 0xfffffffa bytes off the end
                                         * of s->inbuf
                                         */
```

Exploitation

An attacker who can connect to the Asterisk server SCCP "Skinny" port (by default 2000/tcp) can attack the vulnerable function prior to registering as a configured Skinny phone, permitting pre-authentication remote compromise.

Once the initial length header value in the packet performs an integer-wraparound an attacker can overflow off the end of the malloc()ed input buffer, and into heap space above it. Exploitation is possible via standard heap-overflow malloc-unlink-macro technique[1] on glibc versions prior to 2.3.5. On systems with newer glibc, a more sophisticated exploitation method is necessary due to the improved validation of malloc's internal heap management linked lists. Brett Moore's work[2] on bypassing similar restrictions in WinXPSP2 is instructive.

Our proof-of-concept exploit uses vanilla malloc-unlink() to overwrite a GOT entry to point execution back into our buffer, and executes Metasploit port-binding shellcode.

Solutions

- Disable the chan_skinny module if it is not required.
- Firewall port 2000/tcp from untrusted networks.
- Install the vendor supplied upgrades:
  1.0-branch: Upgrade to 1.0.12 or later
  1.2-branch: Upgrade to 1.2.13 or later

Credit

Discovered and advised to Digium 17th October, 2006 by Adam Boileau of Security-Assessment.com.

Security-Assessment.com commends Digium on their extremely rapid response, releasing an updated version within two days of receiving our vulnerability report.

References

[1] "Advanced Doug Lea's Malloc Exploits" by jp
http://doc.bughunter.net/buffer-overflow/advanced-malloc-exploits.html
[2] "Exploiting Freelist[0] On Windows XP Service Pack 2" by Brett Moore
http://www.security-assessment.com/technical/

An attacker who can connect to the Asterisk server SCCP "Skinny" port (by default 2000/tcp) can attack the vulnerable function prior to registering as a configured Skinny phone, permitting pre-authentication remote compromise.

About Security-Assessment.com

Security-Assessment.com is Australasia's leading team of Information Security consultants specialising in providing high quality Information Security services to clients throughout the Asia Pacific region. Our clients include some of the largest globally recognised companies in areas such as finance, telecommunications, broadcasting, legal and government. Our aim is to provide the very best independent advice and a high level of technical expertise while creating long and lasting professional relationships with our clients.

Security-Assessment.com is committed to security research and development, and its team continues to identify and responsibly publish vulnerabilities in public and private software vendor's products. Members of the Security-Assessment.com R&D team are globally recognised through their release of whitepapers and presentations related to new security research.

Security-Assessment.com is an Endorsed Commonwealth Government of Australia supplier and sits on the Australian Government Attorney-General's Department Critical Infrastructure Project panel. We are certified by both Visa and MasterCard under their Payment Card Industry Data Security Standard Programs.
For further information on this issue or any of our service offerings, contact us

Web www.security-assessment.com
Email info@security-assessment.com
Phone +649 302 5093