

# [VulnWatch] apachetop insecure temporary file creation

**Source:** <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2005-09/0017.html>

---

**From:** ZATAZ Audits (*exploits\_at\_zataz.net*)

**Date:** 09/30/05

Date: Fri, 30 Sep 2005 14:17:59 +0200

To: vulldb@securityfocus.com, vuln@secunia.com, vuln@k-otik.com, moderators@osvdb.org, bugs@securi

#####

apachetop insecure temporary file creation

Vendor: <http://clueful.shagged.org/apachetop/>

Advisory: <http://www.zataz.net/adviso/apachetop-09022005.txt>

Vendor informed: yes

Exploit available: yes

Impact : low

Exploitation : low

#####

The vulnerability is caused due to temporary file being created insecurely.

This can be exploited via symlink attacks in combination to create and overwrite arbitrary files with the privileges of the user running the affected script.

#####

Versions:

#####

apachetop <= 0.12.5

#####

Solution:

#####

Apply : apachetop\_CAN-2005-2660.patch

Patch from Steve Kemp (Debian)

<http://bugs.gentoo.org/attachment.cgi?id=69342>

#####

Timeline:

#####

## VulnWatch: [VulnWatch] apachetop insecure temporary file creation

Discovered : 2005-09-02  
Vendor notified : 2005-09-02  
Vendor response : no reponse  
Vendor fix : no patch  
Vendor Sec report (vendor-sec@lst.de) : 2005-09-13  
Disclosure : 2005-09-30

#####

Technical details :

#####

Vulnerable code :

-----

ake a look at : src/apachetop.h

```
247 #define DEBUG_OUTPUT "/tmp/atop.debug"
```

Then in : src/apachetop.cc

```
85 cf.debug = true;
```

```
1103 int dprintf(const char *fmt, ...) /* {{{ */
1104 {
1105 FILE *d;
1106 va_list args;
1107
1108 if (cf.debug && (d = fopen(DEBUG_OUTPUT, "a")))
1109 {
1110 va_start(args, fmt);
1111 vfprintf(d, fmt, args);
1112 fclose(d);
1113 va_end(args);
1114 }
1115
1116 return 0;
1117 } /* }}} */
```

#####

Related :

#####

Bug report : [http://bugs.gentoo.org/show\\_bug.cgi?id=104473](http://bugs.gentoo.org/show_bug.cgi?id=104473)

CVE : CAN-2005-2660

#####

Credits :

#####

Eric Romang (eromang@zataz.net – ZATAZ Audit) – Gentoo security scout  
Thxs to Gentoo Security Team.

[VulnWatch] apachetop insecure temporary file creation